Florida Law Review

Volume 68 | Issue 2 Article 6

January 2017

# Privacy and Common Law Names: Sand in the Gears of Identification

Adam Candeub

# PRIVACY AND COMMON LAW NAMES: SAND IN THE GEARS OF IDENTIFICATION

*Adam Candeub*[*]

## Abstract

During the last two decades, law and regulation have expanded to require real name identification in virtually every aspect of life—from online purchases to healthcare. This slow, subtle transformation has rendered a de facto nullity the Constitution's anonymity protection against compelled identity disclosure. This evolution also has rendered impracticable the traditional, but mostly forgotten, common law rights to use whatever name one wishes—the de facto right to pseudonymity. This common law right facilitates anonymity, which, in turn, facilitates privacy.

This Article argues that the continued vitality of common law name rights, particularly in light of recent First Amendment jurisprudence, establishes a right to pseudonymity. This right includes, in certain circumstances, the ability to demand a government-issued identification under a common law pseudonym. This ability would allow individuals to frustrate regulatory identification regimes and regain some privacy. Beyond these practical implications, this Article, employing the classic property–liability distinction, demonstrates how name governance changed from the common law liability regime to a government-owned property regime. This shift reflects an important, and hitherto unrecognized, transformation in the legal relationship between the state and citizen.

* Professor and Director, Intellectual Property, Information, and Communications Law Program. I wish to thank Jim Harper for his many helpful suggestions. *Pro Julia facio omnes.*

## INTRODUCTION

Not so long ago, Americans led private lives. *The Official Preppy Handbook*, the 1980 satirical Bible of the white Protestant East Coast elite,[1] instructs, "You should appear in print only three times in your

1. *See* Motoko Rich, *Rejoice, Muffy and Biff: A Preppy Primer Revisited*, N.Y. TIMES (Apr. 3, 2010), http://www.nytimes.com/2010/04/04/books/04preppy.html.

life—upon birth, marriage, and death."[2] In 2000, however, Sun Microsystems Inc. CEO Scott McNealy declared that people "have zero privacy anyway" and to "[g]et over it."[3] But a disgruntled preppy might ask—discreetly, of course—"Who killed it?" Who or what is responsible for the major cultural shift?

Many claim technology is to blame. Google, cell phone tracking, mass storage of telephone and internet metadata, mass video surveillance, and cloud storage have made *The Official Preppy Handbook*'s guidelines quaint, if not absurd. The hacked naked photographs of celebrities Jennifer Lawrence, Kim Kardashian, Rihanna, Vanessa Hudgens, and Kate Upton illustrate this cruel reality.[4]

Even the Supreme Court accepts the conventional narrative that technology is privacy's greatest slayer. In its most noteworthy recent privacy and technology decisions, *Kyllo v. United States*[5] and *United States v. Jones*,[6] the Court claimed that its goal is to protect against the "power of technology to shrink the realm of guaranteed privacy."[7]

This Article argues that law, along with technology, has undermined privacy. Specifically, the law of identification has diminished privacy by requiring that individuals use government-issued identification in their everyday transactions. In the last few decades, and particularly since the passage of the REAL ID Act of 2005,[8] most everything people do is subject to identification and subsequent recordation—from opening a bank account or applying for a credit card to receiving healthcare, buying alcohol, or taking an Amtrak train. Cash transactions under $10,000 are probably the only remaining safe harbor.[9]

---

2. LISA BIRNBACH, THE OFFICIAL PREPPY HANDBOOK 25 (1980).

3. Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999), http://archive.wired.com/politics/law/news/1999/01/17538.

4. *See* Stephanie Marcus, *Kim Kardashian's Alleged Nude Photos Leak Online, Many More Celebs Targeted in Hacking Ring (UPDATE)*, HUFFINGTON POST (Sept. 22, 2014, 9:59 AM), http://www.huffingtonpost.com/2014/09/20/kim-kardashian-nude-photo-leak_n_5854634.html (discussing the hacked photographs of Kim Kardashian, Vanessa Hudgens, and Rihanna); Alana Horowitz Satlin & Stephanie Marcus, *Jennifer Lawrence's Nude Photos Leak Online, Other Celebs Targeted*, HUFFINGTON POST (Sept. 2, 2014, 12:59 PM), http://www.huffingtonpost.com/2014/08/31/jennifer-lawrence-nude-photos_n_5745260.html (discussing the hacked photographs of Jennifer Lawrence, Kate Upton, Ariana Grande, and Victoria Justice).

5. 533 U.S. 27 (2001).

6. 132 S. Ct. 945 (2012).

7. *Kyllo*, 533 U.S. at 34; *accord Jones*, 132 S. Ct. at 964 ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

8. REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (codified as amended in scattered sections of 8 and 49 U.S.C. (2012)).

9. *See* Filing Obligations for Reports of Transactions in Currency, 31 C.F.R. § 1010.311 (2015).

The law of identification makes transactions easily attributable to individuals, thereby rendering anonymity and privacy more difficult. Using a false or different name or identity—pseudonymity—to conceal information about oneself is one of the oldest and most powerful ways people hide their identities and retain privacy for the various aspects of their lives. Female authors, such as Jane Austen[10] and Mary Ann Evans,[11] used pseudonymity to preserve their reputation in other spheres of life. Political figures also chose to utilize this tool, such as when James Madison, Alexander Hamilton, and John Jay used the name "Publius" when publishing the *Federalist Papers*.[12] In the landmark case of *NAACP v. Alabama ex rel. Patterson*,[13] the Supreme Court ruled that the First Amendment protects anonymity and pseudonymity—the right against compelled self-identification.[14] Indeed, celebrities continue to rely on the pseudonymity strategy, with Tom Hanks using the name "Harry Lauder" or "Johnny Madrid," Tobey Maguire taking "Neil Deep," and Sarah Michelle Gellar adopting "Neely O'Hara," the name of a character from the novel *Valley of the Dolls*.[15]

Many European countries use, or are beginning to experiment with, official pseudonymous names and numbers in their identification systems.[16] Pseudonymity has particular power online and particular

10. *See* Laura Boyle, *Sense and Sensibility: An Overview*, JANE AUSTEN CTR. (July 17, 2011), http://www.janeausten.co.uk/sense-and-sensibility-an-overview/.

11. Robyn Wagner, Comment, *Don't Shoot the Messenger: Limiting the Liability of Anonymous Remailer Operators*, 32 N.M. L. REV. 99, 103 n.19 (2002) (noting that many famous authors used pseudonyms, including "Mark Twain (Samuel Langhorne Clemens), O. Henry (William Sydney Porter), Voltaire (Francois Marie Arouet), George Eliot (Mary Ann Evans), and Charles Dickens (sometimes writing as 'Boz')").

12. J. Michael Martinez & William D. Richardson, *The Federalist Papers and Legal Interpretation*, 45 S.D. L. REV. 307, 311–12 n.8 (2000).

13. 357 U.S. 449 (1958), *remanded to* 109 So. 2d 138 (Ala. 1959), *rev'd*, 360 U.S. 240 (1959), *remanded to* 122 So. 2d 396 (Ala. 1960).

14. *Id.* at 462 ("Inviolability of privacy . . . may in many circumstances be indispensable to preservation of freedom of association . . . .").

15. Linda Ge, *Sony Hack Exposes Celebrity Aliases for Tom Hanks, Jude Law, Natalie Portman and More in Latest Leak*, WRAP (Dec. 8, 2014, 7:54 PM), http://www.thewrap.com/sony-hack-exposes-celebrity-aliases-for-tom-hanks-jude-law-natalie-portman-and-more-in-latest-leak/.

16. *E.g.*, Niels Vandezande, *Identification Numbers as Pseudonyms in the EU Public Sector*, 2 EUR. J. L. & TECH., no. 2, 2011, at 1, 12 (discussing EU Member States' use of identification numbers as pseudonyms "for the purpose of identifying their citizens in the public sector"); *see also* EUR. CENT. BANK, RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS 3 (2013), https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf (suggesting identification numbers as indicators of a strong customer authentication procedure for internet payments).

importance given the migration of everyday life to the cloud.[17] If data is associated with a pseudonym, then unauthorized release or even sophisticated techniques such as "de-anonymization" of personal data, cannot reveal identity.[18]

Most important, the de facto prohibition of pseudonymity is recent in U.S. law.[19] For most of U.S. history, individuals could use their "common law name," i.e., any name they chose for any reason absent fraud.[20] Individuals could use common law names to make contracts, get married, enter into secured transactions, and open bank accounts—everything required in business and in life. Coupled with a liberal, decentralized government registration scheme, Americans could go through life pseudonymously, and thus anonymously, free from constant identification demands.[21]

This Article examines in detail how the law enabled the emergence of an all-encompassing mandatory identification system that rendered common law names obsolete. The process began in the 1930s with the expansion of government social welfare programs and grew in subsequent years with the social security number (SSN) becoming a standard identifier in government.[22] The SSN also became a standard identifier in private areas such as banking, accelerated by the REAL ID Act of 2005[23], a statute passed in light of 9/11 concerns.[24]

---

17. *See, e.g.*, Mathew Ingram, *Pseudonyms, Trolls and the Battle over Online Identity*, GIGAOM (Jan. 10, 2012, 9:40 AM), https://gigaom.com/2012/01/10/pseudonyms-trolls-and-the-battle-over-online-identity/ (discussing the effects of pseudnoymity on commentary throughout the Internet).

18. *See* Gábor Gy. Gulyás & Sándor Imre, *Analysis of Identity Separation Against a Passive Clique-Based De-anonymization Attack*, INFOCOMMUNICATIONS J., Dec. 2011 11, 12–13, 19.

19. *See infra* Part II.

20. *See* Julia Shear Kushner, Comment, *The Right to Control One's Name*, 57 UCLA L. REV. 313, 316 (2009).

21. *See generally* A. Michael Froomkin, *Anonymity and the Law in the United States*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 441, 442 (Ian Kerr et al. eds., 2009) (discussing the decentralized private law regulation of anonymity).

22. *See Historical Development*, SOC. SEC. ADMIN. 1–2, https://www.ssa.gov/history/pdf/histdev.pdf (last visited Jan. 10, 2016).

23. *See, e.g.*, REAL ID Act of 2005, Pub. L. 109-13, § 202, 119 Stat. 302, 312 (2005) (codified as amended at 49 U.S.C. § 30301 (2012)) (requiring state driver's licenses to include an individual's full legal name for federal recognition); *see also infra* Part II. "REAL ID implements a 9/11 Commission recommendation urging the federal government to 'set standards for the issuance of sources of identification, such as driver's licenses.'" *REAL ID Frequently Asked Questions for the Public*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/real-id-public-faqs (last updated Aug. 19, 2015) [hereinafter *Real ID FAQ*].

24. *See REAL ID Enforcement in Brief*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/real-id-enforcement-brief (last updated Jan. 8, 2016).

The emergence of an endemic, mandatory identification system alters a key legal distinction. The First Amendment does not protect the right to be anonymous but rather the right to be free from government-compelled disclosure of identity.[25] An internet service provider (ISP) must disclose the identity of an "anonymous" poster if served with a subpoena,[26] but the state of Alabama cannot compel citizens to reveal their identity on their political leaflets.[27] Mandatory identification undermines this distinction because it compels one to reveal one's identity all the time: from PayPal and credit card purchases to obtaining a prescription for cold medicine or buying alcohol.

This Article, in a novel analysis, examines the growing, unresolved tensions in case law concerning common law names. As the REAL ID requirements kick in,[28] courts increasingly face the question of whether individuals can demand government-issued identification under their common law names. This Article argues that the common law right and the need for privacy give individuals that power. The government lacks a legitimate interest in a universal identification scheme, as opposed to schemes with limited function, such as the SSN's anti-fraud purpose.[29]

Finally, from a theoretical perspective, this Article adds to the debates about the nature of privacy.[30] This Article argues for a shift from privacy law scholarship's emphasis on defining privacy and arguing its normative or moral dimensions. Instead, this Article underscores the importance of *how* individuals gain privacy in the informational age, i.e., what legal tools people can use to prevent data-mining and de-anonymization. Last, this Article engages in a theoretical analysis of naming, relying on the familiar property–liability rule distinction of Professors Guido Calabresi

25. *See, e.g.*, Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 160, 165–66 (2002) (declaring unconstitutional an ordinance that required registration of those going door-to-door distributing religious printed materials); Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 200 (1999) ("Colorado's current badge requirement discourages participation in the petition circulation process by forcing name identification . . . ."); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 336, 357 (1995) (striking down an Ohio law that prohibited the distribution of anonymous campaign literature).

26. *See infra* note 69 and accompanying text.

27. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–63 (1958), *remanded to* 109 So. 2d 138 (Ala. 1959), *rev'd*, 360 U.S. 240 (1959), *remanded to* 122 So. 2d 396 (Ala. 1960).

28. Jim Harper, *REAL ID: State-by-State Update*, 749 CATO INST. POL'Y ANALYSIS 1, 2 (2014), http://object.cato.org/sites/cato.org/files/pubs/pdf/pa749_web_1.pdf.

29. *See infra* Section III.C. This Article's defense of common law names to facilitate privacy is a proposal allied with other efforts to make personal information gathering more difficult and costly for government and corporation—and was particularly inspired by the work of Professors Finn Brunton and Helen Nissenbaum. *See* FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015).

30. *See infra* Part IV.

and A. Douglas Melamed.[31] This Article shows that the common law naming regime constitutes a liability regime, while the current system of government-issued identification is a property regime where the government, in effect, owns and licenses names. This shift reflects an important, and hitherto unrecognized, change in the legal relationship between the state and citizen.

This Article proceeds as follows. Part I of this Article describes the relationship among common law names, pseudonymity, and privacy. Part II then examines how the gradual expansion of the welfare state, combined with increasing regulation on ubiquitous and necessary industries such as banking and healthcare, has rendered pseudonymity or common law names impractical or illegal. Building on the existing regulation, the REAL ID Act has emerged as the necessary linchpin in a pervasive system of identification. Part III provides the first modern explication of how courts resolve the ongoing tension between a common law name and the variety of statutes that require the use of a formally recognized name. Part III concludes that the common law name, combined with the First Amendment, continues to give individuals in some circumstances the right to demand a government-issued identification under a pseudonym. Finally, using the Melamed–Calabresi framework, Part IV of this Article engages in a theoretical analysis of naming, examining how the shift from the common law liability regime to the current government-owned property regime reflects an unrecognized, dramatic change in the legal relationship between the state and citizen.

## I. PSEUDONYMITY, MANDATORY IDENTIFICATION, AND THE FIRST AMENDMENT

Pseudonymity is one of the oldest and most powerful ways to conceal identity and gain privacy; it creates privacy because actions are not associated with the "real" actor. The First Amendment recognizes the value of anonymous speech and protects it.[32] The First Amendment does so because "to ensure a vibrant marketplace of ideas, some speakers must be allowed to withhold their identities to protect themselves from

31. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972).

32. Margot Kaminski, *Real Masks and Real Name Policies: Applying Anti-mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815, 887–88 (2013) ("[It is] often recognize[d] that anonymity is a First Amendment right or a right closely entwined with free expression. . . . [T]here is a generally common understanding that anonymity is valuable and should in at least some circumstances be protected as a speech right or as an aspect of speech. Even before *McIntyre*, anonymity was thus recognized as a function that has a nexus with free expression, and as a medium for speech that otherwise would not be heard.").

harassment and persecution."[33] Pseudonymity allows the anonymity to travel, purchase items, communicate, and conduct any activity without attribution. Anonymity, in turn, "permits people the fullest range of choice in personal and social development. . . . [and] protects people who engage in dissent, whistle-blowing, and other controversial activities that challenge, and ultimately strengthen, our institutions."[34] Indeed, many legal scholars use anonymity and pseudonymity interchangeably, concluding "pseudonymity is a subset of anonymity."[35]

Leading theorists of modern online communications recognize the importance of anonymity in building internet communities.[36] Beyond anonymity's freeing effect on speech that scholars have observed[37] and have found problematic,[38] pseudonymity can create new types of trust. Judith Donath sees pseudonymity as a "middle ground" where "pseudonymous identities . . . can provide both accountability and privacy."[39]

> [Pseudonyms are] not a lack of integrity, but a feature of being an adaptable person in multiple, [separate] social contexts, understanding the varied mores of the different situations.
>
> . . . .
>
> [P]seudonyms, being local, resembled our physical world experience where time and space effectively carve out separate spheres of interaction. Using one's real name online, on the other hand, collapses contexts, as everything

33. Matthew Mazzotta, Note, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C. L. REV. 833, 833 (2010).

34. JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 90 (2006).

35. *E.g.*, David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 UNIV. CHI. LEGAL F. 139, 154 ("[A] pseudonymous message is an anonymous message, containing no information about the 'actual' identity of the message originator . . . 'banning anonymity'—effectively eliminates all pseudonymous messages as well.").

36. *See, e.g.*, Jason A. Martin & Anthony L. Fargo, *Anonymity as a Legal Right: Where and Why It Matters*, 16 N.C. J.L. & TECH. 311, 331–32 (2015) ("[C]ommunicating anonymously can have a disinhibiting effect on the communicator, freeing that person from societal and individual limitations on expressing her thoughts.").

37. *E.g.*, *id.*

38. *See, e.g.*, Saul Levmore, *The Internet's Anonymity Problem*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 50, 53 (Saul Levmore & Martha C. Nussbaum eds., 2010).

39. Judith S. Donath, *We Need Online Alter Egos Now More Than Ever*, WIRED (Apr. 25, 2014, 2:14 PM), http://www.wired.com/2014/04/why-we-need-online-alter-egos-now-more-than-ever/.

> one has performed or written under that name can be quickly tied together through search.[40]

This Article does not argue that pseudonymity can or should offer *absolute* privacy which would give online child pornographers, online stalkers, and terrorists complete anonymity. Rather, this Article argues that pseudonymity's privacy is relative.[41] If someone checks into a hotel under an assumed name and an acquaintance who works at the hotel recognizes that person, then that person's privacy is destroyed. Similarly, consider a credit card issued to a person's account but with another person's name on it—a perfectly legal arrangement.[42] The shopkeeper who takes the card may identify the person from her face, particularly if she lives in a small town, and certainly an FBI investigator looking at her credit card accounts would see the transaction. But to most store clerks, and all of the store's records, she would be pseudonymous and her purchases, therefore, private. Again, she could be identified, but that would take effort and probably a subpoena. Pseudonymity permits privacy because it throws sand in the gears of the corporate and government mechanisms that identify and track U.S. citizens—it enhances obscurity, raising search costs.[43]

Pseudonymity's relative level of privacy is generally enough, provided the person seeking privacy is not engaging in illegal activities. Precisely where to draw the line is a political question, and as such this Article does not directly address the question. Instead, this Article concerns the *legal mechanisms* that allow or prohibit pseudonymity.

But given the alleged "death of privacy," can pseudonymity matter? The Internet as well as information and communication technologies have transformed the ability of government and industry to gather, search, and use information about citizens and consumers. The U.S. public is well aware of the litany of information-gathering techniques. License plate readers or electronic toll radio-frequency identification (RFID) can identify vehicles and their drivers through DMV databases, thereby

---

40. *Id.*

41. *See id.*

42. *E.g.*, JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 131–32 (2014) (describing Julia Angwin's adaptation of such a technique in her effort to live her life anonymously).

43. *Cf.* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 62 (2009) ("Social networking sites and blogs have increasingly become breeding grounds for anonymous online groups that attack women, people of color, and members of other traditionally disadvantaged classes."); Woodrow Hartzog & Frederick Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1, 4 (2013) ("[I]nformation is obscure online if it lacks one or more key factors that are essential to discovery or comprehension. We have identified four of these factors: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity. . . . Courts could use an obscurity continuum when determining if certain information is eligible for privacy protections.").

allowing the government to keep perfect track of individuals' movements.[44] Mobile telephone companies also can keep track of movements due to the geolocation necessary for cell phone communications, and the government can often obtain these phone records.[45] Soon, drones may keep track of movements as well.[46] Beyond physical movements, computer technology tracks commercial activity, including a person's purchasing habits at the gas station, supermarket, and department stores.[47]

Facebook records in detail data about its users' social networks, disclosing how users arrange the informal aspects of their lives.[48] Google and other search engines keep records of searches, as ISPs, such as Comcast, keep track of every site a person visits.[49] While many people's searches may be trivial, such as whether the local restaurant is open, others can reveal private medical information, major purchases, financial

44. Devlin Barrett, *U.S. Spies on Millions of Drivers: DEA Uses License-Plate Readers to Build Database for Federal, Local Authorities*, WALL ST. J. (Jan. 26, 2015), http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779; Kashmir Hill, *E-ZPasses Get Read All Over New York (Not Just at Toll Booths)*, FORBES (Sept. 12, 2013, 4:44 PM), http://www.forbes.com/sites/kashmirhill/2013/09/12/e-zpasses-get-read-all-over-new-york-not-just-at-toll-booths/.

45. Fabio Arcila, Jr., *GPS Tracking out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 6–7 (2012) ("Among existing (and likely also future) technologies, a great uncertainty exists as to whether the third-party doctrine will allow governments to compel production of user data—including location data—from third-party service providers without a warrant. Technologies subject to the doctrine's reach include GPS devices installed in vehicles by either the owner or manufacturer, either voluntarily or through governmental mandate, as well as the increasingly ubiquitous GPS capabilities of smartphones, all of which involve a third party that provides the GPS service and collects the location data." (footnotes omitted)).

46. Robert Molko, *The Drones Are Coming! Will the Fourth Amendment Stop Their Threat to Our Privacy?*, 78 BROOK. L. REV. 1279, 1312 (2013) (questioning potential limitations for outdoor drone surveillance).

47. Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 4–5 (2011) ("For some time, websites and Internet service providers (ISPs) have been compiling profiles about their customers. . . . And, many consumers would be understandably indignant at the detailed picture of their private lives that profilers possess regardless of how the profilers use the information.").

48. MICHAEL LIEBERMAN, VISUALIZING BIG DATA: SOCIAL NETWORK ANALYSIS 2 (2014), https://c.ymcdn.com/sites/www.casro.org/resource/collection/E0F10496-BE87-48E8-8746-521D403EE4A2/Paper_-_Michael_Lieberman_-_Multivariate_Solutions.pdf.

49. Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 427–28 (2013) ("Companies like Google and AT&T collect large amounts of personal user data from customers. This sort of information was formerly used for marketing and research purposes, but recently the U.S. government has been building national security databases that contain personal user data provided by cooperating telecommunications companies like AT&T." (footnote omitted)).

data, and even sexual desires.[50] Beyond Google, which brags that it saves every search,[51] the government is also keeping track. As with geolocation phone data, the government can easily subpoena information that Google or Comcast stores.[52] And, as the Snowden revelations have shown, the government has gotten into the business big time.[53] Its PRISM program warehouses huge amounts of internet data.[54]

But, one should not underestimate the level of privacy that pseudonymity can provide. Few wish to have perfect privacy; most want just enough. For instance, a person could use a pseudonym to go to the doctor's office without every clerical assistant and office manager or an insurance company knowing about it. Many might find this an important advantage in a small town, and it may in fact persuade a person to get treatment for an embarrassing ailment.

Further, pseudonymity is a valuable weapon against the most technologically advanced tools working against privacy. Consider the concerns about "de-anonymizing data." Many scholars have closely examined the legal and policy implications of de-anonymization.[55]

---

50. *See, e.g.*, Kashmir Hill, *Do These Google Searches Really Reveal Our Deepest Sexual Anxieties?*, FUSION (Jan. 27, 2015, 11:30 AM), http://fusion.net/story/40541/google-searching-our-sexual-shortcomings/; Jose Vilches, *Managing Your Privacy Online: Search Engines*, TECHSPOT (May 28, 2010), http://www.techspot.com/guides/281-manage-search-engine-privacy/.

51. Frida Ghitis, *Google Knows Too Much About You*, CNN (Feb. 9, 2012, 2:58 PM), http://www.cnn.com/2012/02/09/opinion/ghitis-google-privacy/.

52. Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 1, 11–13 (2013) ("The SCA provides that non-content [electronic] records can be compelled through a warrant or court order. . . . 'The government has three options for obtaining communications . . . that have been in electronic storage with an electronic service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d).'" (quoting United States v. Warshak, 641 F.3d 266, 282 (6th Cir. 2010))).

53. *See* Steven R. Morrison, *The System of Domestic Counterterrorism Law Enforcement*, 25 STAN. L. & POL'Y REV. 341, 342 (2014).

54. *See* Michael Greene, *Where Has Privacy Gone? How Surveillance Programs Threaten Expectations of Privacy*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 795, 802 (2014) ("PRISM . . . collects all foreign communications that pass through U.S. hubs."); Ryan W. Neal, *What Can the NSA See? MIT Immersion Project Illustrates Metadata PRISM Can Gather*, INT'L BUS. TIMES (July 10, 2013, 4:24 PM), http://www.ibtimes.com/what-can-nsa-see-mit-immersion-project-illustrates-metadata-prism-can-gather-1340959.

55. *See, e.g.*, Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 99 (2014) ("Not only does Big Data's use have the potential to circumvent existing antidiscrimination regulations, but it may also lead to privacy breaches in health care and law enforcement."); Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1121–22 (2013) ("In the Netflix example, as well as in other prominent examples, anonymization seems not to have worked as intended, and researchers have been able to 'de-anonymize' the data, thereby learning the information of particular individuals from the released data. These examples of de-anonymization have led some

Suppose an epidemiologist obtained data on all individuals receiving treatment for AIDS in a certain county in the United States; the individuals in the sample are identified by zip code, birth date, and sex. Privacy and computer researchers have found that those few nuggets of information often identify one unique individual who could be discovered with a few internet searches.[56] In other words, large numbers of records about an individual likely exist that have been de-anonymized, which could easily be re-identified.

Pseudonyms can protect a person against de-anonymization. Say a person obtains healthcare under a pseudonym with a birth date altered by one day; his anonymity and privacy would remain intact even if his private medical data were released and de-anonymized. In addition, the person's privacy would be protected against casual snoopers in electronic medical records[57] as well as the accidental loss of medical records—apparently a growing problem.[58]

In general, many claim that the data revolution makes obscurity impossible, or at least big data makes privacy through obscurity more difficult.[59] Individuals cannot hide in the sheer mass of data when the

---

to argue that privacy and utility are fundamentally incompatible with each other and that supposedly anonymized data is never in fact anonymous." (footnote omitted)).

56. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1705 (2010) ("How many other people in the United States share your specific combination of ZIP code, birth date (including year), and sex? According to a landmark study, for 87 percent of the American population, the answer is zero; these three pieces of information uniquely identify each of them."); *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1877–78 (2011) ("At some point, a search allows a person to be readily identifiable."); Latanya Sweeney, k-*Anonymity: A Model for Protecting Privacy*, 10 INT'L J. UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYSTEMS 557, 558–59 (2002) ("Combinations of few characteristics often combine in populations to uniquely . . . identify some individuals.").

57. David Schultz, *Medical Data Breaches Raising Alarm*, WASH. POST (June 2, 2012), http://www.washingtonpost.com/national/health-science/medical-data-breaches-raise-alarms/2012/06/02/gJQAVPWt9U_story.html ("As more doctors and hospitals go digital with medical records, the size and frequency of data breaches are alarming privacy advocates and public health officials.").

58. José Luis Fernández-Alemán et al., *Security and Privacy in Electronic Health Records: A Systematic Literature Review*, 46 J. BIOMEDICAL INFORMATICS 541, 542 (2013).

59. *E.g.*, Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 84 (2013) ("Maintaining obscurity will be even more difficult once big data tools, techniques, and datasets become further democratized and made available to the non-data-scientist masses for free or at low cost. Given recent technological trends, this outcome seems to be gradually approaching inevitability."); *see also* Ohm, *supra* note 56, at 1724 (noting the possibility of "combin[ing] anonymized data with outside information to pry out obscured identities"). *But see* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 4 (2011) ("[T]he influential legal scholarship by Ohm and others misinterprets the computer science

government or private entities can easily collect, correlate, and cross-reference.[60] But pseudonymity makes big data less threatening. One can use a pseudonym to ensure that information associated with that pseudonym (what she eats, what she buys, where she goes, what websites she visits) will not be associated with her. It throws sand in the gears of the identification mechanisms.

Of course, anonymity and pseudonymity have costs.[61] For instance, the pseudonymous patient faces inconvenience and possible danger due to medical mistakes resulting from the failure to integrate medical records under both names. However, that is a feature, not a bug. If individuals desire privacy, they must bear the cost. Most people probably would not care enough about privacy to incur the cost, but, for example, an individual with a socially stigmatizing venereal disease who lives in a small, conservative town might.

In this way, pseudonymity can play a major role in throwing sand in the gears, as part of an arsenal of "self-help" privacy. To illustrate, journalist Julia Angwin wrote a book in which she describes her efforts to obtain privacy in today's world.[62] She obtained credit cards under her own account but a different name, used Tor—an anonymizing search engine that masks the identity and location of the user's computer—and refused to use privacy-decreasing technologies.[63] She did not want "perfect" privacy; rather, she just wanted to make it more difficult for the government, data-miners, or anyone else to collect and correlate information about her.[64]

Perhaps most fundamentally, constant identification requirements eliminate First Amendment-protected anonymity.[65] In the last decade, more and more activities in life—from PayPal transactions to receiving healthcare—require identification using a government-issued identification keyed to one's SSN and reflecting one's formal legal name,

literature, and as a result, oversells the futility of anonymization, even with respect to theoretical risk.").

60. Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 414 (2014) ("The growing adoption of big data and its ability to make extensive, often unexpected, secondary uses of personal data changes this calculus. As Kord Davis observed in his book *Ethics of Big Data*, 'the potential for harm due to unintended consequences[] can quickly outweigh the value the big-data innovation is intended to provide.'" (quoting KORD DAVIS & DOUG PATTERSON, ETHICS OF BIG DATA 5 (Julie Steele & Courtney Nash eds., 2012))).

61. This is, of course, equally true on the Internet. For an interesting set of hitherto unidentified costs, see Bryan H. Choi, *The Anonymous Internet*, 72 MD. L. REV. 501, 503–04 (2013) ("[P]reserving [anonymity] will increasingly come at the expense of another attribute [generativity] that is arguably more essential to the Internet's exceptionalism.").

62. ANGWIN, *supra* note 42, at 131–34.

63. *Id.* at 131–34, 188.

64. *Id.* at 127.

65. *See infra* Sections III.C–D.

and even bearing an RFID chip.[66] If an activity requires government-issued identification, then it cannot be done anonymously—and the distinction between compelled identification (protected by the First Amendment) and third-party revealing of identity (not protected) begins to evaporate.

The Supreme Court has long held that the First Amendment prohibits restrictions on anonymous speech, meaning that the government cannot force speakers to identify themselves, particularly when engaging in political, religious, or other protected types of speech.[67] For example, the Court consistently has ruled that the First Amendment prohibits laws requiring individuals engaged in protected speech to identify themselves. On the other hand, courts have held that people have no right to anonymous speech.[68] When speakers identify themselves to ISPs, speakers have no right to demand that the ISP *not* disclose their identifying information.[69]

---

66. *See, e.g.*, *Enhanced Drivers Licenses: What Are They?*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/enhanced-drivers-licenses-what-are-they (last updated Aug. 20, 2015) (discussing the Western Hemisphere Travel Initiative and its recommendation of enhanced driver's licenses).

67. *See* Watchtower Bible & Tract Soc'y, Inc. v. Village of Stratton, 536 U.S. 150, 160, 166–67 (2002) ("For over 50 years, the Court has invalidated restrictions on door-to-door canvassing and pamphleteering."), *remanded to* 42 Fed. App'x 772 (6th Cir. 2002); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995), *remanded to* 650 N.E.2d 903 (Ohio 1995); Talley v. California, 362 U.S. 60, 64–65 (1960) ("Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. . . . It is plain that anonymity has sometimes been assumed for the most constructive purposes."); Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 199–200 (1999) (holding that the First Amendment prohibits a rule that petition circulators wear identification badges because it "compels . . . identification at the precise moment when the circulator's interest in anonymity is greatest"); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–63, 466 (1958) (ruling that state subpoenas seeking the names of NAACP members violate the First Amendment), *remanded to* 109 So. 2d 138 (Ala. 1959), *rev'd*, 360 U.S. 240 (1959), *remanded to* 122 So. 2d 396 (Ala. 1960).

68. *See, e.g.*, First Time Videos, LLC v. Does 1–500, 276 F.R.D. 241, 248 (N.D. Ill. 2011).

69. Most courts apply a balancing test for when ISPs and other networks must reveal identities under civil subpoena. *See* Clay Calvert et al., *David Doe v. Goliath, Inc.: Judicial Ferment in 2009 for Business Plaintiffs Seeking the Identities of Anonymous Online Speakers*, 43 J. MARSHALL L. REV. 1, 26 (2009) ("Courts today generally pay homage to the nation's long history and tradition of protecting anonymous speech, as they tend to apply one of the more rigorous unmasking standards to cases of anonymous Internet speech . . . ." (footnote omitted)). Of course, under the Stored Communications Act and the USA PATRIOT Act, the government has little if any barrier to obtaining metadata and must satisfy a relatively low bar to obtain the content of internet communications. Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 385 (2014) (noting that under the Stored Communications Act, "the government must establish 'specific and articulable facts' to obtain a court order requiring the disclosure of many kinds of noncontent Internet records, such as the to-from addresses on emails"

The constant identification requirement in every aspect of life makes anonymity or pseudonymity impossible—or at least very difficult. After all, the activities that make speech possible—such as writing on the Internet or buying placards—force individuals to identify themselves.[70] Certain political or civil rights groups, such as the National Association of the Advancement of Colored People, have historically faced opposition by racist government officials; anonymity or pseudonymity could protect members and their speech even in a world of constant identification and surveillance.[71] Because anonymity is no longer practicable, pseudonymity offers the best hope for anonymous speech.

## II. HOW THE COMMON LAW NAME DIED

Not too long ago, common law names gave individuals great latitude to use pseudonyms. As discussed below, the common law developed rules for how people could use multiple names to be bound by contract, receive inherited property, marry, and hold secured interests. Even though legislatures never repealed common law names,[72] pseudonymity

---

(quoting Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279, 4292 (1994))).

70. The Internet is not anonymous in that Internet Protocol (IP) addresses are easily traceable to particular broadband lines. Since it is virtually impossible to buy one's broadband connection anonymously, anonymity online is quite difficult. Anonymizer proxy servers such as Tor can provide some anonymity, but even they can be compromised. Dune Lawrence, *The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built*, BLOOMBERG BUS. (Jan. 23, 2014), http://www.bloomberg.com/bw/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency; *see also* Ashley I. Kissinger & Katharine Larsen, *Untangling the Legal Labyrinth: Protections for Anonymous Online Speech*, 13 J. INTERNET L. 1, 16 (2010) ("Legal process seeking the identity of an anonymous poster may arise in various ways. Most frequently, a plaintiff commences a lawsuit against a Jane or John Doe defendant and then moves for issuance of a preservice discovery subpoena on the owner of the Web site on which the offending material was posted, the anonymous poster's Internet service provider (ISP), or both. . . . The subpoena typically requests 'all identifying information' regarding the poster and often identifies that person by the pseudonym under which he or she posted or by the date and time of the post. . . . Because many people register using fake names and non-descript email addresses, the IP address is often the most valuable piece of information sought."). Courts generally apply a balancing test when forcing ISPs or others to "unmask" online actors. *See* Kissinger & Larsen, *supra*, at 19.

71. *Patterson*, 357 U.S. at 462–63 (finding that "on past occasions revelation of the identity of [the NAACP's] rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility," and that anonymity will help protect its members and their right to advocate their beliefs).

72. Leone v. Comm'r, Ind. Bureau of Motor Vehicles, 933 N.E.2d 1244, 1253 (Ind. 2010) ("All states have enacted similar statutes [providing a name change procedure], and all but two have concluded that they do not abrogate but instead supplement the common law."); Kushner, *supra* note 20, 328–29 (noting that "[o]nly a few states have explicitly abrogated the common law

is either illegal or practically impossible in most aspects of life today. The mechanism by which common law names and pseudonymity have been eliminated involves a complicated interaction among consumer regulations, regulated industries, and the criminal law.

First, a list of "true" names had to be created. In the United States, this was not an easy matter because, historically, the several states kept birth records; there was never a readily available national list.[73] The lack of a national registry distinguished the United States from every other industrialized nation of the nineteenth and twentieth centuries.[74] The United States has developed such a list gradually, starting with the social security number (SSN) in the 1930s[75] and culminating with the REAL ID Act of 2005, which finally developed a set of interconnected state databases, cross-referenced by SSNs, that can serve as the official "list"—at least for adults.[76]

Second, there must be a mandate that individuals only use their "official" name. While never formally abandoning the common law name, the United States has created countless regulatory regimes that require the use of government-issued identification. This regulatory web of identification now extends from banking and healthcare to transportation and education.

Third, law and regulation had to outlaw identification other than that with one's official name—or more subtly, the government-issued identification can go "viral," emerging as a sort of standard for all public and private transactions and interactions. Companies and other private entities no longer have to rely on their own methods of identification, as they did under common law regimes, but may piggyback onto the preexisting (and free) government regime.[77]

Ancient common law prerogatives die slow deaths, most often in obscure places shielded from the light of day. Few legislators wish to be known for destroying individual rights. This Part discusses the common law name and registration system as it existed in the eighteenth and nineteenth centuries and how it transformed in the twentieth and twenty-first century.

---

right," while most states have enacted statutes regulating name-change procedures that supplement, rather than replace, the common law).

73. *See infra* Subsection II.B.1.

74. *See infra* Subsection II B.1.

75. Social Security Act, Pub. L. No. 74-271, 49 Stat. 620 (1935) (codified as amended in scattered sections of 42 U.S.C. (2012)).

76. *See* 49 U.S.C. §§ 30301–30304 (2012).

77. In a prophetic article, Professor Michael Froomkin foresaw such a result. Michael Froomkin, *Creating a Viral Federal Privacy Standard*, 48 B.C. L. REV. 55, 84 (2007).

### A. *The Common Law Name, National Registries, and the Unique American System of Identification*

Common law in England and the United States has always permitted common law names. An individual may choose any name he wishes—provided the reasons for requesting the name change are not fraudulent.[78] This name is perfectly legal for all purposes. As a nineteenth-century authority states:

> It is a custom for persons to bear the surnames of their parents, but it is not obligatory. A man may lawfully change his name without resort to legal proceedings, and for all purposes the name thus assumed will constitute his legal name just as much as if he had borne it from birth.[79]

---

78. *See, e.g.*, United States v. Cox, 593 F.2d 46, 49 (6th Cir. 1979); Azeez v. Fairman, 604 F. Supp. 357, 362 (C.D. Ill. 1985) ("The common law name change is valid, however, only if the change does not interfere with the rights of others by serving a fraudulent purpose."), *rev'd*, 795 F.2d 1296 (7th Cir. 1986); United States v. McKay, 2 F.2d 257, 259 (D. Nev. 1924); Christianson v. King County, 196 F. 791, 799 (W.D. Wash. 1912), *aff'd*, 203 F. 894 (9th Cir. 1913), *aff'd*, 239 U.S. 356 (1915); Linton v. First Nat'l Bank, 10 F. 894, 899 n. (W.D. Pa. 1882); Carlisle v. People's Bank, 26 So. 115, 116 (Ala. 1899); *In re* Arnett, 56 Cal. Rptr. 3d 1, 3 n.3 (Ct. App. 2007); *In re* Marriage of Nguyen, 684 P.2d 258, 260 (Colo. App. 1983); Pease v. Pease, 35 Conn. 131, 155 (1868); Reddick v. State, 5 So. 704, 706 (Fla. 1889); Parmelee v. Raymond, 43 Ill. App. 609, 610 (1891); Graham v. Eiszner, 28 Ill. App. 269, 273 (1888); Clark v. Clark, 19 Kan. 522, 524–25 (1878); Stuart v. Bd. of Supervisors, 295 A.2d 223, 226–27 (Md. 1972); Sec'y of the Commonwealth v. City Clerk, 366 N.E.2d 717, 721 (Mass. 1977); Hommel v. Devinney, 39 Mich. 522, 524 (1878); Piotrowski v. Piotrowski, 247 N.W.2d 354, 355 (Mich. Ct. App. 1976); Coplin v. Woodmen of the World, 62 So. 7, 9 (Miss. 1913) ("At common law a man could change his name, in good faith, and for an honest purpose, and adopt a new one, by which he could be generally recognized."); Moskowitz v. Moskowitz, 385 A.2d 120, 122 (N.H. 1978); McGarvey v. Atlantic City, 8 A.2d 385, 387 (N.J. 1939) ("The common law does not prohibit the assumption of any name, unless for a fraudulent purpose, or unless inhibited by a statute or judicial adjudication."); *In re* Pirlamarla, 504 A.2d 1238, 1240 (N.J. Super. Ct. Law Div. 1985) ("The common law permits an adult to change his or her name without leave of court simply by adopting a new name and utilizing it in the ordinary course of daily living."); *In re* Halligan, 46 A.D.2d 170, 171 (N.Y. App. Div. 1974) ("Under the common law a person may change his or her name at will so long as there is no fraud, misrepresentation or interference with the rights of others."); Eisenberg v. Strasser, 768 N.Y.S.2d 773, 776–77 (N.Y. Sup. Ct. 2003), *aff'd but criticized by* 763 N.Y.S.2d 782 (N.Y. App. Div. 2003), *aff'd*, 100 N.Y. 2d 590 (N.Y. 2003); Pierce v. Brushart, 92 N.E.2d 4, 8 (Ohio 1950); Robinovitz v. Hamill, 144 P. 1024, 1025 (Okla. 1914) ("We are satisfied, therefore, that the plaintiff . . . had the right to assume any name under which he chose to conduct his business . . . in good faith, and that he had a right to maintain an action for breach of contracts made under such business name . . . ."); Gearing v. Carroll, 24 A. 1045, 1046 (Pa. 1892); Traugott v. Petit, 404 A.2d 77, 80 (R.I. 1979); Dunn v. Palermo, 522 S.W.2d 679, 688–89 (Tenn. 1975); Kruzel v. Podell, 226 N.W.2d 458, 464 (Wis. 1975).

79. Archibald H. Throckmorton, *Names*, *in* 29 CYCLOPEDIA OF LAW AND PROCEDURE 261, 271 (William Mack ed. 1908).

Similarly,

> At common law a man may lawfully change his name, or by general usage or habit acquire another name than that originally borne by him, and this without the intervention of either the sovereign, the courts, or Parliament; and the common-law rule, unless changed by statute, of course obtains in the *United States*.[80]

Only four states have explicitly abrogated the common law right.[81]

Authorities make clear that common law names need not be limited, i.e., a person could have more than one common law name at once.[82] Thus, common law names could function as perfect pseudonyms. Individuals could effortlessly assume different names in different aspects of their lives.

Further, common law names were legally binding. Under a common law name, one could contract,[83] convey property,[84] be a beneficiary under an insurance contract,[85] get married,[86] inherit property,[87] or be the beneficiary of a negotiable instrument.[88] In short, common law names allowed for pseudonymity in virtually every aspect of life.

---

80. *Name*, *in* 21 THE AMERICAN AND ENGLISH ENCYCLOPAEDIA OF LAW 305, 311 (David S. Garland & Lucius P. McGehee eds., 2d ed. 1902).

81. Kushner, *supra* note 20, at 328–29 n.79 (noting that Hawaii, Louisiana, Maine, and Oklahoma have abrogated the common law name).

82. *See, e.g.*, United States v. Dunn, 564 F.2d 348, 354 n.12 (9th Cir. 1977); Ming v. United States, 103 F.2d 355, 358 (9th Cir. 1939) ("[U]nder the English common law, one may properly have several names."); Burke v. United States, 58 F.2d 739, 741 (9th Cir. 1932) ("[A]n individual, may have, or be known by, more than one name . . . ."); *see also* Hauser v. Callaway, 36 F.2d 667, 669 (8th Cir. 1929) (noting that a person's true name is the one that person is best known by in the community).

83. Schofield v. Jennings, 68 Ind. 232, 235 (1879) ("A person may be known by any name in which he may contract, and in such name he may sue and be sued, and by such name may be criminally punished; and when a person is known by several names—by one as well as another—he may contract in either, and sue and be sued by the one in which he contracts, and may be punished criminally by either. And names which sound alike are held, in law, to be the same, though they may be spelled by different letters.").

84. Wilson v. White, 24 P. 114, 115 (Cal. 1890) ("He may assume a name for the occasion; and a conveyance to and by him under such name will pass the title.").

85. *E.g.*, Everett v. Standard Accident Ins., 187 P. 996, 998–99 (Cal. Dist. Ct. App. 1919).

86. Chipman v. Johnston, 130 N.E. 65, 66–67 (Mass. 1921).

87. *See* Christianson v. King County, 196 F. 791, 792–93, 799 (W.D. Wash. 1912), *aff'd*, 203 F. 894 (9th Cir. 1913), *aff'd*, 239 U.S. 356 (1915) ("In any event, it is well established that a man may lawfully change his name, without resorting to legal proceedings, and for all purposes the name thus assumed by him will constitute his legal name . . . .").

88. Seidman v. N. Camden Tr. Co., 7 A.2d 406, 408 (N.J. 1939) ("The early English cases which first formulated the rule that a bill payable to a fictitious person is by legal intendment

Most importantly, the law developed a system of liability rules to deal with common law names. To borrow Professors Melamed and Calabresi's classic liability–property distinction,[89] a name under common law was an entitlement protected by a liability. Anyone was entitled to use a name, but if one imposed costs on others, one had to pay the cost of using the name. Thus, under the common law, if one used a name for fraud, one had to pay the damages caused.[90]

What is interesting and largely forgotten is that the common law developed fine-tuned liability rules for common law names and pseudonyms. For instance, there were rules for how to treat negotiable instruments made out to pseudonyms or nonexistent persons—they became payable to the bearer.[91] Similarly, the identity of an individual insured under a pseudonym could be discerned through parol evidence.[92] Insurance contracts made under one name for the benefit of a person's other name have been held valid, provided that "you can find it was his intention that he should be known by the name . . . and thereafter retain that name, if you should find that he had to this extent acquired that name, then this representation in the application would not be false."[93] Part IV explores more fully how the current naming regime has become a property entitlement regime.[94]

---

payable to bearer, and may be transferred without indorsement, clearly make the knowledge on the part of the drawer of the fictitious character of the payee a condition of the rule.").

89. *See* Calabresi & Melamed, *supra* note 31, at 1106–07.

90. People v. Porter, 288 P.2d 561, 564 (Cal. Ct. App. 1955); State v. Fick, 464 P.2d 271, 274 (Kan. 1970) ("In our view, defendant falsely made and forged the check. Under the circumstances attendant here, the writing of the Wells's name on the check was false. . . . Defendant did not innocently assume the name of Wells, but opened the account in that name because he had Wells's chauffeur's license to use as a means of identification. Defendant purported to be someone he was not. He attempted to impersonate Darrell D. Wells. He made a deposit of $25, but then promptly proceeded to issue checks against the account, each of which was in an amount exceeding $25. All such conduct was steeped in fraud."); State v. Lutes, 230 P.2d 786, 789 (Wash. 1951) ("After adopting or assuming a name for an honest purpose, its use . . . would not constitute forgery, unless the person using the name falsely assumed it for the purpose and with the intent of perpetrating a fraud.").

91. State v. Weigel, 477 A.2d 372, 377 (N.J. Super. Ct. App. Div. 1984) ("A check which is made payable to a fictitious or nonexistent person is treated as a check made payable to bearer when the maker of the check knows that the payee is either a fictitious or nonexistent person.").

92. Wilson v. White, 24 P. 114, 115 (Cal. 1890) ("So, where a deed was made out in the name of 'James O. Brunius,' and signed, 'J. O. BRUNIUS,' it was held that parol evidence was admissible to show that John O. Brunius was the party who signed the deed, and that if this was proved his title passed.").

93. Smith v. U.S. Cas. Co., 90 N.E. 947, 948 (N.Y. 1910).

94. *See* Calabresi & Melamed, *supra* note 31, at 1092.

## B. *Three Steps to Eliminate the Common Law Name*

As set forth above, destruction of the common law name involves three steps. First, a list of "true" names must be created. Second, law and regulation must develop mandates that individuals only use their "true" name. Third, law and regulation must make any identification bearing any name other than one's official name illegal, and industry practice must require the use of government-issued identification, rendering pseudonymity impractical.

### 1. Step One: Creating a Centralized List of "True" Names in the United States

The United States was unique from its very beginning in having a decentralized name registration, combined with a common law name rule that rendered any centralized naming registry an administrative impossibility.[95] The several states established their own systems for registering births.[96] As described below, it was not until the 1930s that the United States moved toward the European approach and a centralized naming system.

Henry VIII instituted England's first national institution of registration. Using his new power as head of the Church of England,[97] he ordered parishes to keep records of births, deaths, and marriages.[98] The registration lists were to be "a public, local, and civic record, deliberately created . . . for legal and economic purposes."[99] These purposes were primarily inheritance.[100] Thomas Cromwell, Henry VIII's vicar-general, explained the purpose of registration in the following terms: "for the avoiding of sundry strifes, processes and contentions arising from age, lineal descent, title of inheritance, legitimation of bastardy, and for knowledge whether any person is our subject or no."[101] The recording also played a role in government benefit distributions; the Poor Laws,

95. HENRY S. SHRYOCK ET AL., THE METHODS AND MATERIALS OF DEMOGRAPHY 81 (4th prtg. 1980).

96. *Id.*

97. *See* Steven G. Calabresi & Abe Salander, *Religion and the Equal Protection Clause: Why the Constitution Requires School Vouchers*, 65 FLA. L. REV. 909, 976 (2013).

98. Simon Szreter, *The Right of Registration: Development, Identity Registration, and Social Security—A Historical Perspective*, 35 WORLD DEV. 67, 72–73 (2007), http://www.sciencedirect.com/science/article/pii/S0305750X06001811.

99. *Id.* at 67.

100. Simon Szreter, *Registration of Identities in Early Modern English Parishes and Amongst the English Overseas*, *in* 182 PROCEEDINGS OF THE BRITISH ACADEMY: REGISTRATION AND RECOGNITION 67, 71 (Keith Breckenridge & Simon Szreter eds., 2012).

101. EDWARD HIGGS, THE INFORMATION STATE IN ENGLAND: THE CENTRAL COLLECTION OF INFORMATION ON CITIZENS SINCE 1500, at 39 (2004).

early modern England's version of the welfare state, allocated money to beneficiaries according to their recorded status in the parish.[102]

The parish system stopped working well in the early nineteenth century for several reasons. The Industrial Revolution disrupted traditional communities and increased mobility.[103] Also, many dissenting, non-Anglican sects, such as the Quakers, often did not use the parish registries.[104] These changes led to the government's fear that, due to inadequate recordkeeping, the poor could "double dip," receiving benefits at more than one parish.[105]

These shortcomings led to the creation of a national registry office, the General Register Office of England and Wales (GRO),[106] which was a government-run recordkeeping office. While some scholars—notably, Anthony Giddens—have argued that the GRO was created to allow for surveillance, others see the GRO as only continuing the function of ensuring property rights and succession.[107] But despite centralized recordkeeping, England, like the United States, still retained the common law name.[108]

Scandinavian countries relied upon parish recordkeeping, and the church records are quite accurate, extending back to the Middle Ages. Parish records were seamlessly merged with government registries in the nineteenth and early twentieth centuries.[109] This shift occurred in 1924 in Denmark.[110] This transition occurred earlier in Sweden in 1858 when the

---

102. *See id.* at 41–42.

103. *See* Roger Lane, *Crime and the Industrial Revolution: British and American Views*, 7 J. SOC. HIST. 287, 287 (1974).

104. *See General Register Office: Society of Friends' Registers, Notes and Certificates of Births, Marriages and Burials*, NAT'L ARCHIVES, http://discovery.nationalarchives.gov.uk/details/r/C13331 (last visited Nov. 7, 2015).

105. *See* Jane Caplan, *"This or That Particular Person": Protocols of Identification in Nineteenth-Century Europe*, *in* DOCUMENTING INDIVIDUAL IDENTITY: THE DEVELOPMENT OF STATE PRACTICES IN THE MODERN WORLD 49, 56 (Jane Caplan & John Torpey eds., 2001).

106. *See generally* GEN. REG. OFF., http://www.gro.gov.uk/gro/content/ (last visited Jan. 10, 2016) (current GRO website).

107. *Compare* HIGGS, *supra* note 101, at 49–63 (noting that many of GRO's records "reveal such information collection as part of state surveillance but also the creation of rights to property through the official recording of vital events and the will of testators"), *with* ANTHONY GIDDENS, THE CONSEQUENCES OF MODERNITY 57–58 (1990) (arguing that "administrative concentration depends . . . upon the development of *surveillance* capacities").

108. State v. Taylor, 415 So. 2d 1043, 1047 (Ala. 1982) ("[T]he common law of England, that is, that all persons have the right, irrespective of marriage, to use the name or names of their choice so long as the name is not used for a fraudulent purpose.").

109. *See* Karl Jakob Krogness, *Numbered Individuals, Digital Traditions, and Individual Rights: Civil Status Registration in Denmark 1645 to 2010*, 28 RITSUMEIKAN L. REV. 87, 90, 93 (2011).

110. *Id.* at 97.

Central Bureau of Statistics was created; the Bureau, in fact, collected (and still does in rural Sweden) data from church parish records.[111]

France instituted registries as early as 1667 in response to the reforms of the Council of Trent.[112] In 1793, as a result of the French Revolution, recordkeeping was moved from the church to civil registries.[113] In a law dating from the French Revolution, which remained unchanged until 1993, no French person could bear any name but the one in the official registry.[114] No one could change a name except by an official act of the *Conseil d'Etat*, which rarely granted these requests.[115] Even in marriage, neither women nor men could change their name; rather, they adopt a *nom d'usage*. French people can use the *nom d'usage* in all aspects of their lives, but it does not appear on formal legal documents.[116]

Compared to the French and Scandinavian systems, Germany created its registration system much later because it was not unified until 1871.[117] Some smaller German states, particularly those under French influence, employed registration systems.[118] In the February 1875 *Personenestandsgestz*, the unified German state introduced civil registration and created a network of districts and offices.[119] The German central government delegated to the states the power to regulate names and the conditions under which individuals could change their names.[120] The German states adopted consistent rules that greatly resembled the French.[121] In 1895, the great German law authority, Otto Gierke, declared that "a change of family name may [only] be granted by authority of the

111. Ann-Sofie Kälvemark, *The Country that Kept Track of Its Population: Methodological Aspects of Swedish Population Records*, 2 SCANDINAVIAN J. HIST. 211, 214–15 (1977).

112. Caplan, *supra* note 105. The Council of Trent had a huge impact on the recordkeeping of vital statistics in Roman Catholic countries, including marriage statistics. *See* Adam Candeub & Mae Kuykendall, *Modernizing Marriage*, 44 U. MICH. J.L. REFORM 735, 769 (2011).

113. David R. Weir, *New Estimates of Nuptiality and Marital Fertility in France, 1740–1911*, 48 POPULATION STUD. 307, 311 (1994).

114. Loi 6 du 23 août 1794 des noms de famille [Law 6 of August 23, 1794 on family names]. The law of April 1, 1803 (11 Germinal, An XI) confirmed this law. The law did not change until 1993, when a somewhat more liberal approach was adopted. Caplan, *supra* note 105, at 56–57.

115. Caplan, *supra* note 105, at 57.

116. Marie-France Valetas, *The Surname of Married Women in the European Union*, POPULATION & SOCIÉTÉS (Inst. Nat'l d'Études Démographiques), Apr. 2001, at 1.

117. *Issues Relevant to the U.S. Foreign Diplomacy: Unification of German States*, U.S. DEP'T OF STATE, https://history.state.gov/countries/issues/german-unification (last visited Nov. 7, 2015).

118. Caplan, *supra* note 105, at 60.

119. *Id.* at 61.

120. *See id.* at 60.

121. *Id.* at 60–61.

state."[122] Current law has softened this requirement, although name change is still difficult.[123]

In conclusion, if the first step in creating a universal system of identification is the creation of a definitive, centralized list with unique names identifying individuals, then the United States was uniquely behind the curve. Allowing citizens the freedom to adopt names of their choosing without a formal name change—combined with the decentralization of its registration system—rendered any efforts to enforce any identification system fairly impossible. In contrast, France, Germany, and other civil law countries, as well as England, had centralized registries by the nineteenth century. Unlike the continental countries, England did—and still does—have common law names. In the 1930s, the United States, however, shifted toward a European system of identification—and the following section examines that shift.

### 2. Step Two: The Social Security Number and Toward Obligatory Identification

The SSN emerged slowly as a first step to a mandatory identifier. It was only recently—under the REAL ID Act that incorporates the SSNs into driver's licenses[124]—that a complete identification regime emerged. The story of the SSN's emergence demonstrates a "free rider" phenomenon in identification systems. SSNs are very useful not only to governments, but also to private entities.[125] However, they are expensive and difficult to create.[126] Once one identification system is created, there exists a tremendous incentive to "piggyback" onto it and thus make it universal.[127] An identification numbers program's "administrative efficiency . . . encourages government agencies and private firms to adopt national identification numbers."[128]

---

122. *Id.* at 62.

123. *See* BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], art. 10, *translation at* http://www.gesetze-im-internet.de/englisch_bgbeg/englisch_bgbeg.html (Ger.).

124. REAL ID Act of 2005, Pub. L. No. 109-13, § 202, 119 Stat. 302, 312 (codified as amended at 49 U.S.C. § 30301 note (2012) (Improved Security for Drivers' Licenses and Personal Identification Cards).

125. *See* R. Brian Black, *Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models from South Africa and the United Kingdom*, 34 CORNELL INT'L L.J. 397, 398–99 (2001).

126. Carolyn Puckett, *The Story of the Social Security Number*, 69 SOC. SECURITY BULL., no. 2, 2009, at 55, 55–56.

127. *See Historical Background and Development of Social Security*, SOC. SEC. ADMIN., http://www.socialsecurity.gov/history/briefhistory3.html (last visited Nov. 7, 2015) (noting that there were already twenty other nations operating programs similar to Social Security at the time the United States adopted the program).

128. Black, *supra* note 125, at 402.

Congress never passed a law explicitly mandating the SSN. Rather, it empowered the newly created Social Security Administration in 1935 to create an identification system.[129] Politicians at the time provided several assurances that the number would never become a national identifier—and such a claim was plausible given the limited coverage of the early social security system, which excluded most women, African Americans, other minorities, as well as agricultural workers.[130]

The adoption of the SSN outside of the Social Security Administration was gradual.[131] In 1943, President Franklin D. Roosevelt authorized federal agencies to use the number outside of the SSA.[132] While agencies took decades to adopt the SSN as their official identifier, the SSN eventually became indispensable for receiving any government benefits.[133] After the implementation of the SSN in 1936, "its use as an identification number has been congressionally mandated more than forty times."[134]

For example, "[i]n 1961, the Civil Service Commission forced all federal employees to obtain a social security number for use as an employee identification number."[135] The following year, the Internal Revenue Service (IRS) adopted the SSN as an identifier for tax returns.[136] Now, "[t]he Internal Revenue Code stipulates that a SSN is the primary identifying number for individuals who file returns."[137] The U.S. Department of Defense ended the use of service numbers for military personnel in favor of SSNs in 1969.[138] In 1972, legislation gave the Social Security Administration power to assign SSNs to all legally admitted noncitizens at entry and to anyone receiving or applying for federal benefits.[139] In 1973, the Supplemental Security Income program began to

129. Social Security Act, Pub. L. No. 74-271, § 807(b), 49 Stat. 620 (1935) (codified as amended at 42 U.S.C. § 1007 (2012)).

130. Miriam Cohen & Michael Hanagan, *Politics, Industrialization and Citizenship: Unemployment Policy in England, France and the United States, 1890–1950*, *in* CITIZENSHIP, IDENTITY AND SOCIAL HISTORY 91, 122 (Charles Tilly ed., 1996).

131. Black, *supra* note 125, at 411.

132. Exec. Order No. 9397, 3 C.F.R. ch. 2, §§ 283–84 (1943–1948).

133. HARPER, *supra* note 34, at 194–95; *Social Security Number Chronology*, SOC. SEC. ADMIN., http://www.ssa.gov/history/ssn/ssnchron.html (last updated Nov. 9, 2005).

134. Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J.L. & TECH. 319, 350 (2002).

135. Black, *supra* note 125, at 411.

136. *Id.*

137. Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 540 (1998).

138. *Social Security Number Chronology*, *supra* note 133.

139. Social Security Amendments of 1972, Pub. L. No. 92-603, § 137, 86 Stat. 1329, 1364 (codified as amended at 42 U.S.C. § 405 (2012)); *Social Security Number Chronology*, *supra* note

use SSNs.[140] In 1979, Congress required households receiving food stamps to disclose each household member's SSN.[141] In 1981, disclosure of the SSN was required for all adult members of households with children enrolled in the school lunch program.[142] In 1982, all those seeking aid under federal loan programs were required to provide SSNs.[143] In 1984, in an effort to go after "deadbeat dads," the federal government required an alimony payer to furnish the IRS with the SSN of the ex-spouse receiving the payments.[144] Congress, in 1989, required that the National Student Loan Data system include SSNs of borrowers and that the SSNs of the parents of school lunch program applicants be provided.[145] In 1990, Congress required an SSN to obtain Department of Veterans Affairs benefits[146] for each dependent aged one or older claimed by a tax filer[147] and for owners of grocery stores or other establishments that accept food stamps.[148] Congress, in 1994, authorized SSN use for jury selection and federal workers' compensation.[149]

Finally, the 1996 welfare reform legislation required that the SSN appear on numerous official documents, including professional licenses, driver's licenses, death certificates, birth records, divorce decrees,

---

133.

140. *See Chronology: 1970s*, SOC. SEC. ADMIN., https://www.ssa.gov/history/1970.html (last visited Oct. 25, 2015).

141. Food Stamp Act of 1977, Amendment, Pub. L. No. 96-58, 93 Stat. 389, 391 (1979) (codified as amended at 7 U.S.C. § 2025 (2012)).

142. Omnibus Budget Reconciliation Act of 1981, Pub. L. No. 97-35, § 803, 95 Stat. 357, 525 (codified as amended at 42 U.S.C. § 1758); *Social Security Number Chronology*, *supra* note 133.

143. Debt Collection Act of 1982, Pub. L. No. 97-365, § 4, 96 Stat. 1749, 1751 (codified as amended at 26 U.S.C. § 6103 note (2012) (Taxpayer Identifying Number: Persons Applying for Loans Under Federal Loan Programs Required to Furnish)); *Social Security Number Chronology*, *supra* note 133.

144. Deficit Reduction Act of 1984, Pub. L. No. 98-369, § 422, 98 Stat. 494, 797–98 (codified as amended at 26 U.S.C § 215); *Social Security Number Chronology*, *supra* note 133.

145. Student Loan Reconciliation Amendments of 1989, Pub. L. No. 101-239, § 2005, 103 Stat. 2106, 2121 (codified as amended at 20 U.S.C. § 1092b (2012)); *Social Security Number Chronology*, *supra* note 133.

146. Omnibus Budget Reconciliation Act of 1990, Pub. L. No. 101-508, § 8053, 104 Stat. 1388 (codified as amended at 38 U.S.C. § 3001 (2012)).

147. *Id.* § 11,112 (codified as amended at 26 U.S.C. § 6109(e)); *Social Security Number Chronology*, *supra* note 133.

148. Food, Agriculture, Conservation, and Trade Act of 1990, Pub. L. No. 101-624, § 1735, 104 Stat. 3359, 3791–92 (codified as amended at 42 U.S.C. § 405(c)(2)(C)); *Social Security Number Chronology*, *supra* note 133.

149. Social Security Independence and Program Improvements Act of 1994, Pub. L. No. 103-296, §§ 304, 318, 108 Stat. 1464, 1520, 1533 (codified as amended in scattered sections of 42 U.S.C.); *Social Security Number Chronology*, *supra* note 133.

marriage licenses, support orders, and paternity determinations.[150] However, in 1999, Congress repealed the requirement for SSNs to appear on some of these documents, such as driver's licenses and birth records.[151] Blood donations also require SSNs.[152]

Beyond being the required identifier for the federal government, the SSN has also become an essential identifier in state government.[153] In 1976, the federal government authorized the use of SSNs for state taxes, state benefits programs, and motor vehicle registration.[154] While the Intelligence Reform and Terrorism Prevention Act of 2004 (codified at 42 U.S.C. § 405 (2012)) prohibits federal, state, or local governments from displaying SSNs on drivers' licenses, the Real ID Act section 202(d)(5) requires states to verify SSNs when issuing all new drivers licenses—ensuring that the REAL ID Act creates a database of state motor vehicle departments indexed by social security number.[155] Further, under some circumstances the federal government can disclose tax return information—which includes the SSN—to state enforcement authorities.[156] Unsurprisingly, state and federal records in the National Crime Information Center (NCIC) also include SSNs.[157]

Of course, the SSN is also a tool to track private market transactions. As pointed out above, the efficiencies and ease of using an established identification regime are tremendous, as private entities can "piggyback" onto established identification regimes without expending the cost of creating their own regime. And, by the 1970s, the SSN became a tool for tracking private financial transactions.[158]

---

150. Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, § 317, 110 Stat. 2105, 2220–21 (codified as amended at 42 U.S.C. § 666(a)); *Social Security Number Chronology*, *supra* note 133.

151. *Social Security Number Chronology*, *supra* note 133.

152. Komuves, *supra* note 137, at 538.

153. *See Social Security Number Chronology*, *supra* note 133.

154. Tax Reform Act of 1976, Pub. L. No. 94-455, § 1211, 90 Stat. 1520, 1711–12 (codified as amended at 42 U.S.C. § 405); *Social Security Number Chronology*, *supra* note 133.

155. *See* TODD B. TATELMAN, CONG. RESEARCH SERV., RL32722, INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004: NATIONAL STANDARDS FOR DRIVERS' LICENSES, SOCIAL SECURITY CARDS, AND BIRTH CERTIFICATES 4, 7 (2005).

156. *See* 26 U.S.C. § 6103(c) (2012). The current version of the statute allows the disclosure of parts of a return for numerous other reasons. *Id.* Disclosure of "return information," which includes the SSN, is more limited but includes child support enforcement and student loan default collection. *See id.* § 6103(l)(6)–(m)(4).

157. Komuves, *supra* note 137, at 542 ("In addition to the federally-maintained NCIC file, state-maintained law enforcement records are also keyed to SSNs."); *see also* Privacy Act of 1974; Modified System of Records, 60 Fed. Reg. 19,774, 19,776–77 (Apr. 20, 1995) (authorizing the FBI to add names and identifying data of members of violent criminal gangs and terrorist organizations to the NCIC's information).

158. *See id.* at 67–68.

The move towards the SSN as a financial identifier started slow. In 1964, the U.S. Department of Treasury began to require buyers of Series H savings bonds to submit their SSNs; in 1973, the Treasury extended this requirement to buyers of Series E savings bonds.[159] More importantly, in 1970, Congress passed laws requiring banks, savings and loan associations, credit unions, and securities dealers to obtain the SSNs of all customers[160]—a requirement that the USA PATRIOT Act later strengthened.[161] In 1983, this requirement was extended to all interest-bearing accounts held by any institution.[162] Finally, as part of its money laundering laws, Congress required persons engaged in a trade or business to file a report including an SSN to the IRS for cash transactions over $10,000.[163]

The pervasiveness of the SSN requirements for financial information led to its use in financial records, beyond those uses that Congress or statute required. For instance, credit reports use SSNs.[164] Additionally, "most banks and lending institutions use the [SSN] as the method of identifying certain persons."[165] Similarly, the SSN is often the unofficial personal identifier for all healthcare information as well as professional licenses issued by accrediting organizations.[166]

---

159. SOC. SEC. ADMIN., REPORT TO CONGRESS ON OPTIONS FOR ENHANCING THE SOCIAL SECURITY CARD at app. B (1997), https://www.ssa.gov/history/reports/ssnreportap.html.

160. *See* Federal Deposit Insurance Act, Amendments, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended in scattered sections of 5, 12, and 15 U.S.C.); *Social Security Number Chronology*, *supra* note 133.

161. *See* International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, Pub. L. No. 107-56, § 326, 115 Stat. 296, 317 (codified as amended at 31 U.S.C. § 5318) (outlining requirements for accountholder verification and identification).

162. Interest and Dividend Tax Compliance Act of 1983, Pub. L. No. 98-67, § 104, 97 Stat. 369, 371–76 (codified as amended at 26 U.S.C. § 3406); *Social Security Number Chronology*, *supra* note 133.

163. 31 C.F.R. §§ 1010.311–12 (2015) (requiring a financial institution to report on a Currency Transaction Report "the name and address of the individual presenting a transaction" that exceeds $10,000, and "the identity, account number, and the social security or taxpayer identification number . . . of any person . . . on whose behalf such transaction [was] . . . effected").

164. *Credit Reporting Basics: How Private Is My Credit Report?*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/how-private-my-credit-report (last updated June 2015).

165. Komuves, *supra* note 137, at 537 (alteration in original) (quoting Jeffrey A. Taylor, *Medical Process Patents and Patient Privacy Rights*, 14 J. MARSHALL J. COMPUTER & INFO. L. 131, 141 n.75 (1995)).

166. *See* Mike Miliard, *Without a UPI, Healthcare Awash in SSNs*, HEALTHCARE IT NEWS (Oct. 23, 2014, 3:20 PM), http://www.healthcareitnews.com/news/without-upi-healthcare-awash-ssns; *Credit Reporting Basics*, *supra* note 164.

### 3. Step Three: The REAL ID Act of 2005 and Criminalizing Pseudonymity

After creating a definitive registry and mandating its use, the third step requires making false or pseudonymous identification either illegal or impracticable. The REAL ID Act of 2005 played a central role in achieving this result,[167] mandating that the states create identification cards that are unique and associated with the holder's SSN.[168] Thus, it is legally impossible to obtain state identification under any name that is *not* the same as the one registered with the Social Security Administration. At the same time, the government and private industry, in a plethora of different areas ranging from healthcare to banking, require a "government-issued" identification, which typically means an identification card compliant with the REAL ID Act.

Making misrepresentations illegal involves a complicated nexus of laws. Most of the laws are meant to prevent fraud in government benefits, such as the prohibition against misstating one's SSN.[169] Some involve the need to track taxable income, as with the Bank Security Act's requirement on identification of interest-bearing accounts and brokerage accounts.[170] Others, such as the prohibition on false identification cards, seem simply to enforce registration requirements.[171]

Rather than describe these laws, the following Subsections present several scenarios to demonstrate how laws and, in particular, the regulatory and business schemes that have developed around the SSN have made pseudonymity impossible.

#### a. Healthcare

Many individuals would wish to have healthcare provided confidentially. A person's health affects others' views of that person. For instance, many would wish to keep private mental illness or erectile dysfunction. Business people may not wish to share details about their health, as it might affect potential clients from entering into long-term relations.

---

167. *See* REAL ID Act of 2005, Pub. L. No. 109-13, § 202, 119 Stat. 302, 312 (codified as amended at 49 U.S.C. § 30301).

168. 6 C.F.R. § 37.11(e) (2015) ("[I]ndividuals presenting the identity documents listed in § 37.11(c)(1) and (2) must present his or her Social Security Administration account number card; or, if a Social Security Administration account card is not available, the person may present any of the following documents bearing the applicant's SSN . . . .").

169. *See* 18 U.S.C. § 1028 (2012) (prohibiting fraud in connection with identification documents).

170. 31 C.F.R. § 1020.410 (2015) (requiring banks to create and maintain additional records).

171. *See, e.g.*, 18 U.S.C. § 1028.

Congress recognized this desire for privacy when it passed the Health Insurance Portability and Accountability Act (HIPAA), a rather strange "law." Section 264(a) of HIPAA requires the Secretary of Health and Human Services (HHS) to make "recommendations on standards with respect to the privacy of individually identifiable health information" within twelve months of HIPAA's enactment date.[172] Section 264(b) explains that these recommendations must address "at least" the following issues:

> (1) The rights that an individual who is a subject of individually identifiable health information should have.
>
> (2) The procedures that should be established for the exercise of such rights.
>
> (3) The uses and disclosures of such information that should be authorized or required.
>
> Section 264(c) states that if Congress should fail to enact legislation governing "standards with respect to the privacy of individually identifiable health information" within 36 months of the enactment of HIPAA, HHS shall promulgate "final regulations" containing such privacy standards not later than 42 months after the enactment of HIPAA.[173]

Congress never passed such protections, so HIPAA is largely a regulation.[174]

172. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 264(a), 110 Stat. 1936, 2033 (codified as amended at 42 U.S.C. § 1320d-2 note (2012) (Recommendations with Respect to Privacy of Certain Health Information)).

173. Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dep't of Health & Human Servs., 224 F. Supp. 2d 1115, 1120 (S.D. Tex. 2002) (citation omitted) (quoting HIPAA § 264(b)–(c)), *aff'd*, 67 F. App'x 253 (5th Cir. 2003).

174. *See, e.g.*, Modifications to the HIPAA Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164 (2015)).

As many commentators agree, HIPAA regulation has failed to protect patient privacy[175] and, in fact, stymies medical research.[176] One commentator asserts that "HIPAA [is] a fig leaf—or worse, as kudzu choking off the free flow of information."[177]

A pseudonym could provide some help. Suppose a person wished to secure his data against de-anonymization or simply from nosy secretaries and other hospital employees in his small town. This person could receive healthcare under a pseudonym, with a slightly altered date of birth. Instead of John Doe, born November 14, 1980, he is Jonathan Davidfreund, born November 20, 1980. This difference would not affect medical advice or treatment, as the age difference of six days could not affect a medical diagnosis or treatment remedy. All the data related to the treatment—a Caucasian male, birth date November 20, 1980, in the zip code 19075—would be associated with a pseudonym.[178]

The following discussion shows how regulations working with the REAL ID Act make such a strategy impossible under any method of healthcare payment.

Government-Sponsored and Private Insurance Programs. With government insurance (Medicare or Medicaid), pseudonymity is virtually impossible. The government is paying benefits and requires the use of the SSN and the formal legal name. And, if someone attempts to use a different name, there are countless statutes she may be violating that involve false statements.[179]

---

175. *E.g.*, Joshua D.W. Collins, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 201–02 (2007) ("While HIPAA imposes a host of obligations on covered entities in an attempt to increase patient privacy, it does not explicitly create any individual rights for patients affected by medical privacy violations. . . . Lack of medical record protection does not just harm those whose privacy is violated."); Kendra Gray, *The Privacy Rule: Are We Being Deceived?*, 11 DEPAUL J. HEALTH CARE L. 89, 118 (2008) ("The Privacy Rule is not working. Something must be changed to ensure that our personal health information is being protected and that the health care industry has an incentive to obey the law."); Daniel J. Oates, *HIPAA Hypocrisy and the Case for Enforcing Federal Privacy Standards Under State Law*, 30 SEATTLE U. L. REV. 745, 776 (2007) ("Problems with information privacy have become exponentially more pronounced in the last decade. The privacy protections in HIPAA have proven insufficient to protect patient's rights.").

176. Ohm, *supra* note 56, at 1769–70.

177. Susannah Fox, *HIPAA's Broken Promises*, HEALTH CARE BLOG (Sept. 27, 2009), http://thehealthcareblog.com/blog/2009/09/27/hipaas-broken-promises/ (quoting Paul Ohm).

178. *See supra* Part I.

179. *See, e.g.*, 18 U.S.C. § 371 (2012) (prohibiting conspiracy to defraud the United States); *id.* § 1001 (prohibiting false statements generally); *id.* § 1002 (prohibiting possession of false papers); *id*. § 1027 (prohibiting false statements and concealment of facts); *id.* § 1028 (prohibiting fraud and related activity in connection with identification documents); *id.* § 1031 (prohibiting major fraud against the United States); *id.* § 1035 (prohibiting false statements relating to healthcare); 42 U.S.C. § 3795a (2012) (prohibiting falsification or concealment of facts for federal assistance).

But, what if she has employer-provided private insurance? While the law may not explicitly prohibit an individual from using a common law name, numerous laws and recent regulations require insurance companies, employers, and healthcare providers to obtain formal, legal names found in government-issued identification. The REAL ID Act, combined with recent regulations under the Affordable Care Act or industry requirements,[180] makes the use of a driver's license or other government-issued identification necessary. Since she cannot obtain a government-issued identification under a pseudonym, she is practically, if not legally, forbidden from obtaining employer-provided healthcare under a pseudonym.

Employer-Provided Health Insurance. To claim insurance for an employee, the employer would have to report to the IRS the health benefits it paid on the employee's behalf and would use an SSN—otherwise it would have to pay tax on the amounts expended to purchase the employee's insurance.[181] If there were an audit, employers would have to show that benefits were being extended to an actual person.

While it might be theoretically possible for an employer to keep records documenting that it is purchasing insurance for an employee under a pseudonym, the employer would bear a significant cost and risk of legal liability from a host of laws, including making false statements to Medicare[182] and the Wire Fraud Act.[183] Nonetheless, even if an employee were able to have his employer purchase health insurance for him under an assumed name, he would have additional problems from his private insurance company and healthcare provider.

Insurance Company Coverage. Group health insurance companies must provide SSNs so that Medicare can coordinate payments with other health benefits.[184] This ensures that people with two kinds of insurance do not "double dip." It seems likely that insurance companies would have issues with persons whose SSN matched with another name on file with the government. In short, given the legal liability that insurance

180. *See* NAT'L IMMIGRATION LAW CTR., FREQUENTLY ASKED QUESTIONS: IMMIGRANTS, TAXES, AND THE AFFORDABLE CARE ACT 1–2 (2015), https://www.nilc.org/document.html?id=115; *Employer-Provided Health Coverage Informational Reporting Requirements: Questions and Answers*, INTERNAL REVENUE SERV., https://www.irs.gov/uac/Employer-Provided-Health-Coverage-Informational-Reporting-Requirements:-Questions-and-Answers (last updated Sept. 2, 2015).

181. *See* 26 U.S.C. § 162(a) (2012) (providing for deductibility of trade or business expenses).

182. *See* Medicare, Medicaid, and SCHIP Extension Act of 2007, Pub. L No. 110-173, § 111, 121 Stat 2492, 2497–99 (codified as amended at 42 U.S.C. § 1395y(b)) (describing liabilities incurred for failure to follow the Act).

183. 18 U.S.C. § 1343 (2012) (prohibiting fraud by wire, radio, or television).

184. Medicare, Medicaid, and SCHIP Extension Act § 111.

companies face concerning obligations to obtain correct information, insurance companies would likely not issue cards with a common law name.

Direct Payment to Healthcare Providers. Providers must adopt policies to prevent identity fraud under the so-called 2007 "Red Flags Rule" of the Fair and Accurate Credit Transactions Act of 2003, which amended the Fair Credit Reporting Act.[185] These include the presentation of government-issued identification; Congress limited the scope of these regulations to exclude many healthcare providers.[186] Nonetheless, to prevent identity fraud, many insurance companies still require providers to obtain identification.[187] Thus, corporate policies would likely require government-issued identification, which must match one's SSN. It would be illegal to have duplicate identifications—one with a pseudonym or an identification that did not match one's SSN.

Payment with Cash. If one wishes to maintain anonymity by paying with cash, presumably that person would not need to deal with installment payments, and the Red Flags Rule would not apply. But, again, practicality limits the effectiveness of this strategy. First, few people with serious or chronic illnesses could afford such a strategy. Second, large medical systems are unlikely to make exceptions to their anti-identity fraud programs.

Payment to Pharmacist. Finally, consider a person who is able to find a provider that does not require identification. Her healthcare provider takes cash and she uses a pseudonym. She is diagnosed with a sinus infection and obtains a prescription for an antibiotic, which she takes to the pharmacist. At last, she thinks, she can obtain anonymous healthcare! However, under state laws designed to prevent individuals from abusing prescription drugs, she very well may have to provide a driver's license at the pharmacy where she fills her prescription.[188] And do not even think

185. Pub. L. No. 108-159, § 112, 117 Stat. 1952, 1955–57 (2003) (codified as amended at 15 U.S.C. § 1681c-1 (2012)).

186. In 2009, the U.S. District Court for the District of Columbia ruled that the application of the Red Flags Rule's definition of creditor was too broad. *See* Am. Bar Ass'n v. Fed. Trade Comm'n, 671 F. Supp. 2d 64, 70, 88 (D.D.C. 2009) (discussing the Red Flags Rule's related answers on the Commission's "Frequently Asked Questions" website), *vacated as moot* 636 F.3d 641 (D.C. Cir. 2011). Congress later changed the law to limit the scope of the Red Flags regulations. Chris Dimick, *Red Flags Clarification Exempts Most, Not All Providers*, J. AHIMA (Dec. 16, 2010), http://journal.ahima.org/2010/12/16/red-flag-clarification-exempts-most-not-all-providers/.

187. *See, e.g.*, BlueCross BlueShield of ILL., BLUE REVIEW FOR CONTRACTING INSTITUTIONAL AND PROFESSIONAL PROVIDERS 6 (2014), http://www.bcbsil.com/pdf/education/bluereview/june_14.pdf.

188. According to a recent survey, the following states have identification review to obtain prescription drugs: Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Nevada, New Mexico, New York, North

about using fake identification; both federal and state law prohibit possessing a fake ID, let alone using one to procure prescription medicine.[189]

### b. Pseudonymous Purchases and Financial Transactions

"I shop therefore I am"—or so says post-modern artist Barbara Kruger.[190] Few matters are more personal or more defining than what people buy and where people put their money. Cash allows for anonymous purchasing as well as storage of wealth. After the purchase, there is no record of what a person bought. Similarly, no entity keeps track of cash held by individuals—up to a point. Cash transactions over $10,000 cannot be anonymous; rather, those involved must submit a report.[191]

While some degree of anonymity is possible when using cash, the following shows that anonymity is impossible if any portion of personal wealth is in any other form or if the person conducts any other type of transaction. This shortcoming renders anonymous online purchases and financial transactions virtually impossible. Additionally, the pattern that destroyed anonymity in healthcare works the same way in financial transactions: the government creates regulations that require entities to

---

Carolina, North Dakota, Oregon, South Carolina, Texas, Vermont, Virginia, and West Virginia. *See* CONN. GEN. STAT. § 20-612a (2015); 24 DEL. ADMIN. CODE § 5.1.10 (2013); FLA. STAT. § 893.04 (2015); GA. CODE ANN. § 26-4-80 (2015); HAW. REV. STAT. § 329-41 (2015); IDAHO ADMIN. CODE r. 27.01.01.464 (2015); 720 ILL. COMP. STAT. 570/312 (2015); IND. CODE § 35-48-7-8.l(b) (2015); LA. STAT. ANN. § 40:971(E) (2015); ME. STAT. tit. 32, § 13795 (2015); 105 MASS. CODE REGS. 700.001, .012 (2015); MICH. ADMIN. CODE r. 338.3102, .3162 (2015); MINN. STAT. § 152.11 (2015); NEV. REV. STAT. § 453.431 (2015); N.M. CODE R. § 16.19.20.42 (LexisNexis 2015); N.Y. COMP. CODES R. & REGS. tit. 10, §§ 80.73–.74 (2015); N.C. GEN. STAT. § 90-106.1 (2015); N.D. ADMIN. CODE 61-04-03.1-01 (2015); OR. ADMIN. R. 855-019-0210 (2015); S.C. CODE ANN. § 44-53-360 (2015); TEX. HEALTH & SAFETY CODE ANN. § 481.074 (West 2015); VT. STAT. ANN. tit. 18, § 4215b (2015); VA. CODE ANN. § 54.1-3420.1 (2015); W. VA. CODE R. § 60A-3-308 (2015); *see also* CTRS. FOR DISEASE CONTROL & PREVENTION, MENU OF STATE PRESCRIPTION DRUG IDENTIFICATION LAWS 2 (2013), http://www.cdc.gov/phlp/docs/menu-pdil.pdf (reporting that twenty-five states allow pharmacists to request identification before filling a prescription order).

189. *See* 18 U.S.C. § 1028 (prohibiting fraud and related activity in connection with identification documents, authentication features, and information); U.S. DEP'T OF JUSTICE, REGULATORY STRATEGIES FOR PREVENTING YOUTH ACCESS TO ALCOHOL: BEST PRACTICES 27 (2011), https://www.ncjtc.org/PIRE/ES/TOOLBOXforEnvironmentalStrategies/Relevant%20Documentation%20and%20Resources/Publications/RegulatoryStrategiesPublication.pdf.

190. Ron Rosenbaum, *Barbara Kruger's Artwork Speaks Truth to Power*, SMITHSONIAN MAG. (July 2012), http://www.smithsonianmag.com/arts-culture/barbara-krugers-artwork-speaks-truth-to-power-137717540/?no-ist.

191. 31 U.S.C. § 5313(a) (2012) (requiring a financial institution to report transactions regulated by the Secretary of the Treasury); 31 C.F.R. §§ 1010.311–12 (2015) (requiring a financial institution to report a Currency Transaction Report).

request information, including government-provided identifications.[192] And, as Professor Michael Froomkin points out, these identifications can go "viral."[193]

Start with opening a bank account or applying for a credit card, or even a PayPal account.[194] Section 326 of the USA PATRIOT Act[195] requires certain financial institutions to have a Customer Identification Program (CIP).[196] This statutory requirement led the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the U.S. Department of Treasury to jointly issue regulations.[197] These regulations require that the bank verify the customer's name, date of birth, residential or business street address, and identification number.[198] The regulations make clear that for U.S. citizens, a bank must obtain a U.S. taxpayer identification number—for example, an SSN, individual taxpayer identification number, or employer identification number—to open an account.[199]

The CIP regulations prescribe certain methods and documents for verifying this information.[200] For individuals, these documents may include "unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard."[201] In addition to documentary evidence, the CIP allows for non-documentary evidence for the purpose of determining whether "there is logical consistency between the identifying information provided, such as the customer's name, street address, ZIP code, telephone number, date of birth, and social security number (logical verification)."[202]

Thus, while the CIP regulations do not provide explicit instructions, as banking institutions must simply make "reasonable" efforts to determine customers' identities, its "suggestions" provide safe harbors

192. *See, e.g.*, 31 C.F.R. §§ 1010.311–12.

193. Froomkin, *supra* note 77, at 56.

194. *PayPal's Customer Identification Program (CIP) and Its Benefits*, PAYPAL, https://www.paypal.com/us/webapps/helpcenter/helphub/article/?solutionId=FAQ734 (last visited Sept. 15, 2015).

195. Pub. L. No. 107-56, § 326, 115 Stat. 272, 317 (codified at 31 U.S.C. § 5318A(b)(1)(B)).

196. 31 C.F.R. § 1010.220.

197. *See id.* § 1010.100(r), .350.

198. *Id.* § 1020.220(a)(2)(i)(A).

199. *Id.* § 1020.220(a)(2)(i)(A)(4).

200. *Id.* § 1020.220(a)(2)(ii).

201. *Id.* § 1020.220(a)(2)(ii)(A)(1).

202. Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090, 25,100 (May 9, 2003) (codified at 31 C.F.R. § 1010.220).

that banks will likely apply.[203] These safe harbors all have the driver's license or other government-issued identification anchored in them.[204] Failure to follow the CIP regulations can lead to severe criminal and civil penalties,[205] as well as expulsion from the banking profession.[206]

Until the last few decades or so, one could open a bank account under a pseudonym with some difficulty, but over the last few years it has become almost impossible.[207] It would require essentially lying about one's SSN, an illegal act.[208] Or, one could use fake identification, but this again is illegal.[209] In short, the common law right has evaporated.

Naturally, these laws exist to assist law enforcement in uncovering money laundering, child pornography, terrorism, and tax evasion.[210] But they have the effect of baring all private financial transactions naked to the state. Technology does play a role here in that it facilitates the collection of this information, but it is the law that is doing most of the work.

Some scholars argue that modern banking would be impossible under anonymous or pseudonymous accounts, even if relying upon modern cryptographic techniques.[211] Perhaps. But, as discussed above, the common law has developed simple rules to address pseudonymity in secured transactions, inheritance, and negotiable instruments.[212] These rules do not provide perfect anonymity, but they provide enough for the parties involved and seem to have worked well enough.

Finally, at one time, banks—mostly in Switzerland and other tax havens such as Andorra and the Channel Islands—offered numbered accounts, which were pseudonymous.[213] Each client had a number, and

---

203. *See* 31 C.F.R § 1020.220(a)(2).

204. *Id.* § 1020(a)(2)(ii)(A).

205. *See* 31 U.S.C. § 5321 (2012) (describing civil penalties); *id.* § 5322 (describing criminal penalties).

206. *See, e.g.*, 12 U.S.C. § 1818(e)(2) (2012).

207. *See* Streber, *Numbered and Pseudonym Accounts*, STREBER WEEKLY (May 15, 2014), https://www.streber.st/2014/05/numbered-and-pseudonym-accounts/.

208. 18 U.S.C. § 1028.

209. *Id.*

210. *See* 31 C.F.R. § 1010.301 (tax evasion); *id.* § 1010.520(b) (money laundering and terrorism); Deborah L. Morgan, Note, *Digital Signatures: Will Government Registration of Users Mean that Anonymity in Transactions on the Internet Is Forever Lost?*, 2004 U. ILL. L. REV. 1003, 1005 (2004) (child pornography).

211. *E.g.*, Peter Swire, The Uses and Limits of Financial Cryptography: A Law Professor's Perspective (Aug. 15, 1997) (unpublished manuscript), http://www.peterswire.net/archive/pscrypto.html.

212. *See supra* Section II.A.

213. *Numbered Bank Account*, SWISS PRIVACY, http://www.swiss-privacy.com/numbered-bank-account.html (last visited Oct. 25, 2015) ("Numbered bank accounts are offered by Swiss banks to the majority of their clients."); Streber, *supra* note 207 (noting Andorra is a jurisdiction

the bank had no record of who owned the assets.[214] To make a withdrawal or deposit, clients simply presented a secret number.[215] In the United States, the Foreign Account Tax Compliance Act of 2010[216] essentially made these accounts illegal for Americans.[217] This law places considerable disclosure duties on American taxpayers who have overseas accounts, and pseudonymous ownership is considered an indicium of a willful violation.[218]

Abandoning all identification requirements for banking is not desirable and certainly not politically palatable,[219] but the gradual erosion of individual rights should make one hesitate. One can gain significant anonymity in financial transactions simply by incorporating and having a corporation make those purchases.[220] This is a relative type of privacy that could be very useful: vendors will not know with whom they are dealing, although the bank and the IRS will. But this system would be expensive and impractical for most.[221] On the other hand, pseudonymous financial transactions would be available to more people, and making

---

that allowed pseudonymous bank accounts); Arden Dale, *Tax Havens Shift as Luxembourg Loosens Bank Secrecy*, WALL ST. J.: TOTAL RETURN (Apr. 10, 2013, 3:03 PM), http://blogs.wsj.com/totalreturn/2013/04/10/tax-havens-shift-as-luxembourg-loosens-bank-secrecy/ ("[The] Channel Islands . . . are favorite destinations for some who want to keep money below the radar of tax authorities and out of sight of the world in general.").

214. Streber, *supra* note 207.

215. *Id.*

216. Pub. L. No. 111-147, 124 Stat. 97, 97–117 (codified as amended in scattered sections of 26 U.S.C. (2012)).

217. *See* Laura Saunders, *What Offshore Account Holders Need to Know About the Credit Suisse Plea*, WALL ST. J.: MONEYBEAT (May 20, 2014, 8:01 AM), http://blogs.wsj.com/moneybeat/2014/05/20/what-offshore-account-holders-need-to-know-about-the-credit-suisse-plea/ (stating that "foreign financial institutions will begin the process of reporting income information about their account holders who are U.S. taxpayers to the IRS . . . or face severe consequences").

218. *Id.* ("Evidence of willfulness could include having an account in a country with bank-secrecy laws, such as Switzerland; not disclosing the account to your tax preparer; having a numbered account or one held under a pseudonym; [or] having undeclared income of about $5,000 or more a year . . . .").

219. Morgan, *supra* note 210, at 1018 (stating that "[a]ctual anonymity may not be realistic or desirable in all cases"); *see also* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 479 (1996) ("In light of these possibilities, even if they are largely theoretical, it would not be surprising if many governments, including the U.S. government, wish to act to discourage or forbid the issuance and use of completely anonymous digital cash, at least forms that allow it to be exchanged in denominations higher than those proposed by Mondex.").

220. Allen Applbaum et al., *Corporate Anonymity*, FTI J. (Apr. 2013), http://www.ftijournal.com/article/corporate-anonymity.

221. *See* Carol Tice, *The Cost of Incorporation*, ALLBUSINESS, http://www.allbusiness.com/the-cost-of-incorporation-1650-1.html (last visited Nov. 10, 2015).

them completely inaccessible impinges upon privacy that Americans once enjoyed.

## III. GOVERNMENT-ISSUED IDENTIFICATION VERSUS THE COMMON LAW: THE DEVELOPING CASE LAW

The United States' de facto abolition of the common law name turns heavily upon the mandatory use of government-issued identification, primarily the driver's license. The importance of the pervasiveness of government-issued identification cannot be overstated. It has become viral and could create the database of doom, which can record everything about everyone—a possibility that Professor Paul Ohm has decried (and descried).[222] Such a mechanism seems far-fetched. But when identification is required—to make purchases, travel, buy alcohol, use a credit card, open a bank account—and that identification has consistent identifying information, such as name and SSN, then the outlines of such a database emerge.

If one could obtain pseudonymous government identification, one could open bank accounts, receive healthcare, and buy alcohol under a pseudonym, which would evade the potential of the all-encompassing identifiers. Indeed, this is not an absurd idea. As mentioned above, many European countries are experimenting with such approaches.[223]

However, the U.S. common law and the First Amendment may provide the right of individuals to demand that the government recognize their common law names. The pivotal position of government-issued identification creates a very interesting chicken-and-egg question. If common law name rights exist and the purpose of state identification is simply to record a name, it would seem that one might have a right to a government-issued identification. After all, the purpose of government identification is to identify a name, and the individual has the power to determine her name under common law.[224]

The response is that, as some courts have held, neither the common law name right nor a First Amendment right to one's name is a fundamental right.[225] In other words, the right to name oneself is neither an enumerated right in the Bill of Rights incorporated through the Fourteenth Amendment nor one of the few un-enumerated rights, such as travel and marriage, that the Court has read into the Fourteenth Amendment.[226] Therefore, the government may reasonably regulate

222. *See* Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug. 23, 2012), https://hbr.org/2012/08/dont-build-a-database-of-ruin.

223. *See supra* note 16 and accompanying text.

224. *See supra* Section II.A.

225. *See infra* Sections III.B–C.

226. *See infra* Section III.B.

naming by requiring documentation of legal name changes,[227] prohibiting the use of pseudonym,[228] and issuing state identification only upon the meeting of certain criteria.[229]

An answer to this response might be that identification is necessary to engage in actions that are fundamental rights, such as the rights to marry or to travel. These rights are meaningless if one cannot exercise them under one's name. In other words, one's fundamental right to marriage includes a right to be married under one's "true" or even "pseudonymous" name.[230]

Other courts *have* recognized, at least in the prison context, a First Amendment right to make the government recognize a common law name.[231] Thus, one could argue that the right to naming is fundamental, perhaps proceeding from the First Amendment's right to speech and the Fourth Amendment's right to privacy.

The case law is divided, inconsistent, and undeveloped—although this may change as the burdensome requirements of the REAL ID Act begin to kick in[232] and as individuals with inadequate documentation find themselves unable to get any identification and seek court redress.[233] The cases point to several contradictions. On one hand, in today's age, the common law name right is meaningless—as is the concomitant anonymity it can provide—unless one can obtain government-issued identification under a common law name. Similarly, there are cases that do lend some support for the notion that the common law name right does receive some First Amendment protection.[234]

The best way to reconcile these cases would involve a First Amendment inquiry using intermediate scrutiny to examine the government's refusal to grant common law name identifications. Intermediate scrutiny is appropriate because restrictions on what names go on government-issued identification are content neutral, i.e., the restrictions do not apply to any specific names.

A government law or regulation satisfies intermediate scrutiny if "it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression;

227. *See* Puckett, *supra* note 126, at 66.

228. *See* Morgan, *supra* note 210, at 1018.

229. *See, e.g.*, N.Y. STATE DEP'T OF MOTOR VEHICLES: ID-44 (2015), http://dmv.ny.gov/forms/id44.pdf (form for proofs of identity).

230. *See infra* Section III.D.

231. *See infra* Section III.C.

232. Press Release, U.S. Dep't of Homeland Sec., DHS Provides Updates on REAL ID Enforcement (Oct. 9, 2015), http://www.dhs.gov/news/2015/10/09/dhs-provides-updates-real-id-enforcement.

233. *Cf. REAL ID FAQ*, *supra* note 23.

234. *See infra* Section III.C.

and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest."[235] Applying intermediate scrutiny, it would be essential to identify what "important or substantial governmental interest" refusing common law names furthers.[236] Presumably, the governmental interest is a pervasive identification regime, which is *not* an important or substantial governmental interest. Rather, the government might have an interest to ensure that in specific instances—for example, airplane travel or receipt of benefits—identity must be assured. But, there is no need for a comprehensive identification regime to achieve this end. As this Article discusses below, and as is being introduced in Europe, individuals can have different names in different contexts. And, perhaps, as Jim Harper suggests, identification can be delegated to private entities, not the state.[237]

The following discussion examines the cases involving individuals requesting common law names on government-issued identification, canvassing the various approaches courts have taken. It concludes that a right exists to demand government-issued identification under certain circumstances.

### A. *Common Law Names Are Legal Names: The Government Must Simply Duly Record*

Cases concerning name changes are perhaps the most obvious example of states following the principle that individuals are masters of their name—and the state must simply record their desires. During the 1970s, conventions about women's married and divorced names were rapidly changing.[238] Courts ruled that women were free to decide what names to use;[239] the state had no business imposing its views about what married or divorced women should call themselves;[240] and state agencies had to issue identification papers consistent with women's wishes.[241] In reaching these conclusions, courts often relied upon the ancient common

235. Turner Broad. Sys., Inc. v. Fed. Commc'ns Comm., 512 U.S. 622, 662 (1994) (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

236. *See id.*

237. *See* HARPER, *supra* note 34, at 244–45.

238. Omi Morgenstern Leissner, *The Name of the Maiden*, 12 WIS. WOMEN'S L.J. 253, 258 (1997) (describing the 1970s movement "advocating women's right to name themselves").

239. *See, e.g.*, Custer v. Bonadies, 318 A.2d 639, 641 (Conn. Super. Ct. 1974).

240. *See, e.g.*, *In re* Lawrence, 337 A.2d 49, 52 (N.J. Super. Ct. App. Div. 1975).

241. *See, e.g.*, *Custer*, 318 A.2d at 641 ("We live in the age of the women's rights movement . . . . It hardly seems the time for the Connecticut courts to accept an outdated rule of common law requiring married women to adopt their spouse's surnames contrary to our English common-law heritage and to engraft that rule as an exception to the recognized right of a person to assume any name that he or she wishes to use.").

law naming right.[242] Again, this is a distinction between a common law country and civil law country, where there is an official registry of names and formal rules as to what individuals may call themselves.[243]

The U.S. Department of State's policy for issuing passports follows the principle that the common law controls. According to regulation, a person must demonstrate nationality and identity to obtain a passport.[244] To establish nationality, one usually submits a birth certificate.[245] To establish identity, one typically submits a previous or current U.S. passport book; previous or current U.S. passport card; driver's license (not temporary or learner's license); Certificate of Naturalization; Certificate of Citizenship; military identification; or federal, state, or municipal government employee identification card.[246] As an alternative method to establish one's identity for a passport, someone who lacks documentary evidence can appear with a witness who can identify her and state that he has known her for at least two years.[247] Presumably, such a witness could identify the person under her common law name.

Courts have upheld not only this approach but also the principle that individuals are entitled to a passport in their own common law name. In *United States v. Cox*,[248] the court dealt with an alleged violation of the law against falsifying information submitted in passport applications because Cox used a common law name.[249] The court ruled that applicants can use common law names in such applications provided the state in which the applicant resides recognizes common law names.[250]

Presumably, a person could use his common law name passport to open a bank account and, thereby, do business with some anonymity. But there would be complications if one attempted to obtain other types of identification. In particular, obtaining a driver's license under the REAL ID Act requires consistency between the SSN and the name,[251] while

242. *See, e.g.*, *id.* (holding that "the common-law right of a person to the use of a name . . . applies to the surname of a married woman"); *In re Lawrence*, 337 A.2d at 52 ("We conclude that, in circumstances such as here where the husband consents to his wife's resumption of her maiden name, the denial of plaintiff's application was without warrant under N.J.S.A. 2A:52-1 or common law and thus an abuse of the trial judge's discretion.").

243. *See supra* Subsection II.B.1.

244. *First Time Applicants*, U.S. DEP'T OF STATE, http://travel.state.gov/content/passports/en/passports/first-time.html (last visited Nov. 10, 2015).

245. *Id.*

246. *Id.*

247. *Secondary Evidence of Identification*, U.S. DEP'T OF STATE, http://travel.state.gov/content/passports/english/passports/information/secondary-evidence1.html (last visited Nov. 10, 2015).

248. 593 F.2d 46 (6th Cir. 1979).

249. *Id.* at 48.

250. *Id.* at 49.

251. *See* 49 U.S.C. § 30301 note (2012) (Minimum Issuance Standards).

opening a bank account under the CIP rules requires banks to identify inconsistencies among identifying documents.[252] Further, it still would be illegal to use a different SSN on a passport, thus limiting the effective anonymity.[253]

### B. *The Government Has No Obligation to Recognize the Common Law Name*

One legal approach to the common law name right allows people to use the name in any context but concludes that the government has no obligation to issue identification or even recognize a common law name change. Under this approach, the government is only obligated to recognize a formal name change. Of course, as shown above, without a government-issued identification with a pseudonym, the common law name is useless in today's world.[254]

The alternative legal view starts with the assumption that the common law name right is not fundamental.[255] Therefore, government regulation of its use must only be reasonable or rational.[256] As explained above, fundamental rights are typically those enumerated rights in the Bill of Rights incorporated through the Fourteenth Amendment.

A typical example of this approach is the Indiana Supreme Court's decision in *Leone v. Commissioner, Indiana Bureau of Motor Vehicles*,[257] which ruled on whether an individual could demand a common law name on his driver's license.[258] The court reasoned as follows:

> The General Assembly required an application to include a person's name, birth date, and Social Security number, indicating it anticipated the Bureau might verify identities using these points of data. The Social Security Administration is as logical an anchor as any to accomplish

252. *See supra* text accompanying notes 200–06.

253. *See* I.R.C. § 6039E (2012) (requiring an applicant to provide an SSN, if one exists, when applying for a U.S. passport or renewal of a U.S. passport).

254. *See supra* text accompanying notes 225–30.

255. Brown v. Cooke, 362 F. App'x 897, 900 (10th Cir. 2010) ("[T]he district court concluded that 'there is [no] fundamental right of citizens to compel the Government to accept a common-law name change and reform its records accordingly.' We agree with this conclusion, but the substantive due process analysis requires further inquiry. If a proper substantive due process challenge to Colorado's identification card statutes was before the district court, the court would have been required to examine those statutes under the rational basis test."); Jorgensen v. Larsen, 930 F.2d 922, 1991 WL 55457, at *3–*4 (10th Cir. 1991) (unpublished table decision) (holding that the plaintiff had no protected liberty interest in the use of her birth name on her Utah driver's license).

256. *Jorgensen*, 1991 WL 55457, at *3.

257. 933 N.E.2d 1244 (Ind. 2010).

258. *Id.* at 1255.

> this end. In light of the section's requiring an application to include a Social Security number and the Bureau's responsibility to verify its records, there is no doubt that the statute allows the Bureau to use Social Security records to verify Appellants' identities.
>
> If Appellants' position about the statute held sway, drivers could change their names through the common-law method and demand their license reflect that change without taking any formal actions with the agencies that maintain their records. Like it or not, the Social Security Administration has become the custodian of Americans' basic identifying information, and almost all state governments rely on this information to verify identities. In light of this reality, the Bureau has logically decided to verify the identities of those with licenses and identification cards with the Social Security Administration.[259]

The sweep of this opinion is breathtaking. The whole point of the common law name is that individuals can use it "without taking any formal actions with the agencies that maintain their records."[260] With a sigh of indifference, the court declares that "the Social Security Administration has become the custodian of Americans' basic identifying information."[261] The court had it exactly backwards. Individuals choose their names, not vice versa, and one dissenting judge made this precise point in *Jorgensen v. Larsen*.[262]

Indeed, subsequent courts have stepped back from *Leone.* For example, *Worley v. Waddell*[263] demonstrates the logical and constitutional infirmity of the purported principle that no fundamental rights are involved in the right that the government recognize one's common law name.[264] Because Worley, through no fault of his own, had inconsistent names on his birth certificate and file with the SSA, he could not receive a driver's license. The facts are compelling:

> Plaintiff . . . was born to an unwed mother . . . in July 1968. His birth certificate issued at the time identified him as "Joseph Alan Ivey." In 1969, Plaintiff's mother married his biological father and . . . [registered him with the Social

259. *Id.* at 1254–55 (citations omitted).

260. *Id.* at 1255.

261. *Id.*

262. 1991 WL 55457, at *6 (10th Cir. 1991) (McKay, J., dissenting) ("Moreover, Utah law requires applicants to use their 'legal name.' The appellant's 'legal name' may very well be her maiden name. (No one has proved the contrary.) But the Driver License Division will not allow her to use it. I believe this is irrational.").

263. 819 F. Supp. 2d 826 (S.D. Ind. 2011).

264. *Id.* at 830.

> Security Administration] under the name "Joseph A. Worley," which is the name he has used ever since. [And, thus, "Joseph A. Worley" is a common law name. Worley] has repeatedly applied to the Indiana Bureau of Motor Vehicles ("BMV") for a photo ID or driver's license that would enable him to vote, to obtain a marriage license, legally change his name, and/or proceed with the adoption of his child. The BMV has denied his successive applications, however, because the name associated with his social security number does not match the name on his birth certificate. The Social Security Administration has also refused to issue Plaintiff a new card due to his lack of a state-issued photo ID.[265]

The court ruled in favor of Worley. Conceding that under *Leone* there is no fundamental right to demand a government-issued identification, the court stated that individuals have a fundamental right to do all the things that require government-issued identification,[266] which, as this Article shows, is pretty much everything.

But did the court simply defend the fundamental rights to marry, travel, and vote? It would seem that there is a strong logical implication that the *Waddell* court actually vindicated a right to name oneself, i.e., to marry, travel, and vote under a common law name. While the court said it was simply allowing Waddell an identity, the court vindicated the identity that Waddell chose—his common law name. Would the court have ordered the Indiana Bureau of Motor Vehicles (BMV) to give Worley a driver's license that said "Joseph Alan Ivey"—a name that was his "legal" name on his birth certificate but which he disclaimed?

In other words, one could read this case as arguing that the government cannot deny individuals an identity—and that is it. But, if one would be uncomfortable resolving the matter by issuing a mandamus order to the Indiana BMV to issue a driver's license in the name of "Joseph Alan Ivey," then the court's holding cannot be so simple. Rather, the logical conclusion is that there is some basic right in naming oneself. Or, at least, if the common law name right means anything, it must entail some obligation of the government to recognize the individual's name of choice.

### C. *First Amendment Rights to Government Recognition of Common Law Names*

Beyond the conceptual problem of whether the government can, in effect, tell people what to call themselves, the First Amendment also protects a right to demand that the government recognize a common law

265. *Id.* at 827–28 (citations omitted).

266. *Id.* at 830.

name. However, the First Amendment analysis is strangely bifurcated. In the penal context, courts have found a fundamental right to call oneself what one wishes.[267] Many courts have ordered prison authorities to use and recognize common law names—at least names for which there is no formally recognized name change. As the U.S. Court of Appeals for the Fifth Circuit ruled, "[t]he adoption of Muslim names by inmates practicing that religion is generally recognized to be an exercise of both first amendment speech and religious freedom."[268] In other words, in the prison context, some courts have recognized a First Amendment right to make the government recognize one's common law name. In contrast, members of the public generally do not have a fundamental right to have the government recognize or record chosen names, as the *Leone* case discussed above suggests.

The First Amendment right to force the government to recognize one's common law name while incarcerated is often limited because full enjoyment of that right is "inconsistent with [prisoners'] status [in] . . . the corrections system."[269] Courts consequently have placed restrictions on the ability of inmates to change their names. Circuit courts differ on the degree to which the religious or common law right is recognized by correctional institutions, with some, such as the U.S. Court of Appeals for the Ninth Circuit, being broad[270] and others, such as the U.S. Court of Appeals for the Seventh Circuit, being quite limited.[271]

For instance, some courts have required prisons to use "a/k/a" for prisoners.[272] Other courts have required inmates to use formal name change procedures.[273] These disparities result in part from the change in

267. *See, e.g.*, Felix v. Rolan, 833 F.2d 517, 518 (5th Cir. 1987) (holding that the First Amendment protects an inmate's use of a religious name).

268. *Id.* Many courts have ruled that an inmate has a First Amendment interest in using his religious name, at least in conjunction with his committed name. *E.g.*, Salaam v. Lockhart, 905 F.2d 1168, 1170 (8th Cir. 1990); Barrett v. Virginia, 689 F.2d 498, 502 (4th Cir. 1982); Fawaad v. Herring, 874 F. Supp. 350, 352 (N.D. Ala. 1995), *aff'd sub nom.* Fawaad v. Jones, 81 F.3d 1084 (11th Cir. 1996). Some courts only consider whether a name was adopted for religious reasons and do not consider whether the name would be protected for expressive reasons. *See* Ali v. Stickman, 206 F. App'x 184, 186 (3d Cir. 2006).

269. Salahuddin v. Coughlin, 591 F. Supp. 353, 359 (S.D.N.Y. 1984) (quoting Pell v. Procunier, 417 U.S. 817, 822 (1974)).

270. *E.g.*, Malik v. Brown, 71 F.3d 724, 729 (9th Cir. 1995) (recognizing that "prisons are required to take simple measures to accommodate prisoners' First Amendment rights").

271. *See, e.g.*, Mutawakkil v. Huibregtse, 735 F.3d 524, 526–27 (7th Cir. 2013); Azeez v. Fairman, 795 F.2d 1296, 1298–99, 1302 (7th Cir. 1986).

272. *E.g.*, *Felix*, 833 F.2d at 519.

273. *See, e.g.*, Salaam v. Lockhart, 905 F.2d 1168, 1175 (8th Cir. 1990) ("The policy of the Department of Corrections with respect to its records thus far exceeds in its scope the administrative interests recognized by state law. The a/k/a alternative which permits continued

Supreme Court precedent, which limited a once-broader protection of prisoners' constitutional rights.[274]

*Azeez v. Fairman*[275] reflects a parsimonious take on a prisoner's right to a common law name.[276] Abdullah Muhammad sought to have the prison's records changed to reflect his common law name.[277] He argued that as Illinois recognizes common law names, the Department of Corrections must reflect his common law name in official records.[278] The Department of Corrections refused to recognize the plaintiff's name.[279]

Judge Richard Posner sided with the Department of Corrections.[280] He reasoned that because naming is not a fundamental right, the state may reasonably require a formal name change to alter his records.[281] His reasoning was in keeping with the cost–benefit analysis characteristic to his jurisprudence.[282] He asserted that a name change's cost to the Department of Corrections was significant.[283] He envisioned the wardens being constantly bombarded with name change requests.[284]

Judge Posner's analysis would have an interesting application to non-imprisoned individuals. In contrast to imprisoned individuals, non-imprisoned individuals have no diminishment of rights, and there are no prison wardens to be bombarded with notices of name changes. Thus, the benefits seem greater and the costs significantly less. The balance would seem to tip in the favor of common law rights. Importantly, cases such as *Leone* do not even engage in such balancing.

---

use of committed names in prison records as Arkansas requires demonstrates the unreasonableness of the current practice.").

274. *See* Turner v. Safley, 482 U.S. 78, 87 (1987) ("In none of these four 'prisoners' rights' cases did the Court apply a standard of heightened scrutiny, but instead inquired whether a prison regulation that burdens fundamental rights is 'reasonably related' to legitimate penological objectives, or whether it represents an 'exaggerated response' to those concerns.").

275. 795 F.2d 1296 (1986).

276. *See id.* at 1296, 1298–99, 1302.

277. *Id.* at 1297. The named plaintiff, Azeez had legally changed his name. Muhammad was a co-plaintiff and simply adopted a new name after his conversion to Islam. *Id.*

278. *Id.*

279. *See id.* at 1298.

280. *Id.* at 1302.

281. *Id.* at 1299.

282. *See id.* at 1298–99, 1301.

283. *Id.* at 1298.

284. *Id.* at 1298–99; *see also* Rahman v. Stephenson, 626 F. Supp. 886, 888 (W.D. Tenn. 1986) ("The *Salahuddin* case is precisely on point, and its reasoning is compelling."); Salahuddin v. Coughlin, 591 F. Supp. 353, 359 (S.D.N.Y. 1984) ("Common-law name change, even for religious purposes, is among the rights that plaintiffs lost as 'inconsistent with their status as prisoner[s] of the corrections system.'" (alteration in original) (quoting Pell v. Procunier, 417 U.S. 817, 822 (1974))).

### D. *The First Amendment, Intermediate Scrutiny, and Government-Issued Identification*

Assume *arguendo* that the First Amendment implies some level of scrutiny for government refusal to provide identification under a common law name. Concededly, no court has so ruled outside of the prison context. On the other hand, the few cases that have touched on the matter failed to address the prison cases. More importantly, the strange inconsistencies of the *Waddell* case show that government-issued identification certainly can implicate fundamental rights.[285]

That there should be some First Amendment right to demand identification in one's common law name seems evident from this Article's analysis. Government-issued identification plays an inescapable role in determining the name that individuals must use in banking, business, and healthcare—virtually all aspects of life. If one retains a meaningful right to use whatever names one wishes, one must have the right, at least in some circumstances, to have government-issued pseudonymous identification.

So assume there is some First Amendment requirement to have the government issue an individual identification under a common law name. As such, courts should review restrictions on government-issued identification under First Amendment intermediate scrutiny. This level of judicial scrutiny is appropriate for content-neutral time, place, and manner restrictions. Requiring REAL ID-conforming identification is a classic content-neutral regulation because it prohibits all types of names, not certain types with an objectionable content. Such a requirement is, in a way, a time, place, and manner restriction. Most of the time, individuals can call themselves whatever they wish but may not do so when they travel, go to the doctor, buy a bottle of wine, or open a bank account.

A government law or regulation will satisfy intermediate scrutiny if "it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest."[286] This inquiry leads to the question set forth above, central to this Article. What is the governmental interest in a pervasive identification regime? Again, given that the United States survived for so long without one, it is hard to see what one might be. While there is certainly a governmental interest in establishing identities in certain contexts, such as government benefits and airports and border crossings, this does not imply an interest in a comprehensive regime.

---

285. *See supra* Section III.B.

286. Turner Broad. Sys. Inc. v. Fed. Commc'ns Comm'n, 512 U.S. 622, 662 (1994) (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

On this point, it is interesting to look at the stated purpose of the REAL ID Act. The REAL ID Act has a stated "official purpose" that "includes but is not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine."[287] In its implementing regulations, the Department of Homeland Security (DHS) accepted those purposes and did not add any.[288] Even the linchpin of the current identification regime does not claim to be a comprehensive identification regime.

The issue of purpose leads to the second part of the intermediate scrutiny analysis: the incidental restriction on alleged First Amendment freedoms must be no greater than is essential to the furtherance of that interest. If one disaggregates the governmental interests from a generalized universal identification regime into distinct instances where the government has an interest in identity, then less restrictive approaches become apparent. Consider the governmental interest in preventing fraud in benefits. Here, common law or pseudonymous names can reasonably be restricted in the obtaining of benefits. Unique identification cards should be issued for social security benefits, Medicare, Medicaid, and all other government benefits. However, these identities could be specific to the government program. Individuals could establish identity using their "real names" but then use pseudonyms for receiving government benefits, once they established identity. While the government may have records cross-referencing identities, these need be neither public nor shared with other parts of the government. European governments and Australia are experimenting with this approach.[289]

In addition, the government has an interest in security. Border control and airplane traffic are areas where the government has a legitimate interest in establishing identity. Again, one could establish a pseudonymous identity for the purpose of obtaining a passport. Alternatively, as Jim Harper has argued, private entities could take on the job of identification.[290] Indeed, they already have.[291] For instance, ClearMe identification is currently used at major airports throughout the

287. REAL ID Act of 2005, Pub. L. No. 109-13, § 201(3), 119 Stat. 302, 312 (codified as amended at 49 U.S.C. § 30301 note (Improved Security for Drivers' Licenses and Personal Identification Cards)).

288. Minimum Standard for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. 5272, 5277 (Jan. 29, 2008).

289. Vandezande, *supra* note 16, at 12; OFF. OF THE AUSTRALIAN INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLE GUIDELINES: PRIVACY ACT 1988, ch. 2, at 2 (2014), https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf.

290. HARPER, *supra* note 34, at 244–45.

291. *Id.*

United States.[292] It is a private firm that contracts with airports to provide security.[293] Individuals pay for the service, which offers expedited security.[294] To receive the service, individuals give their fingerprints and retina scans to ClearMe, which then clears the individuals with the Transportation Security Administration.[295] These biometric identifiers provide easy transit through security.[296] But, the trick is that ClearMe contractually obligates itself to reimburse individuals against any privacy breaches; yet there is no reason why ClearMe could not issue its identification under a pseudonym as it relies on biometric markers.[297]

## IV. WHAT'S IN A NAME? A THEORETICAL ANSWER

This Article describes a dramatic shift in the law of the name—from common law to a comprehensive identification regime under the REAL ID Act. This transformation presents the question: what is the legal status of a personal name? Despite the vast literature on intellectual property interests in a name, there is no comparable scholarship on personal names. For instance, a trademark is like property. It belongs to the entity who uses it or to whom it has been legally transferred.[298] Businesses can receive court injunctions to prevent others from using it, just as one could receive an injunction for someone presenting a nuisance to real property. But, what about personal names?

Professors Calabresi and Melamed's landmark article[299] created the standard theoretical model for understanding property and liability rules,

292. *See Where Is Clear?*, CLEARME, http://www.clearme.com/where-is-clear (last visited Nov. 10, 2015) (describing ClearMe as currently available at twelve U.S. airports).

293. HARPER, *supra* note 34, at 235.

294. *Id.* at 235–36.

295. *Id.* at 235.

296. *Id.* at 235–36.

297. *Id.*

298. 3 LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMPETITION, TRADE, & MONOPOLIES ("But the incorporeal nature of a trademark tends to obscure its substantiality. Property is a multifaceted and evasive term, more philosophical than legal in meaning and extent. In legal parlance it connotes the right to exclude others from any use, or from disturbing the owner's use, thereof. The right of a trademark owner with respect to his mark is (or should be) the right to be protected with respect to all three functions, i.e., as an indication of the common origin of all products and services offered under the mark.").

299. Calabresi & Melamed, *supra* note 31; *see also* Carol M. Rose, *The Shadow of* The Cathedral, 106 YALE L.J. 2175, 2175 (1997) ("*One View of the Cathedral* is now so much a part of the legal canon that it is widely known simply by the joined names of its two authors, 'Calabresi and Melamed.' In turn, 'Calabresi and Melamed' has become a shorthand name for the article's most famous legacy: the distinction between 'property rules' and 'liability rules' as means of protecting entitlements." (footnote omitted)).

which "represent alternatives for enforcing a legal entitlement."[300] Property rules govern entitlements that require consensual access.[301] Outsiders cannot enter private property without the owner's consent; if they do, the owner can get an injunction from a court.[302] Or, the owner may elect to charge outsiders for the privilege.[303] In contrast, liability allows for nonconsensual access and requires an objective payment.[304] Anyone may publicly perform a copyrighted song without the copyright holder's permission, provided that they pay an established licensing fee. Or, similarly, risky drivers may crash into other drivers and interfere with their entitlement to have an undamaged car, provided the risky driver is willing to pay objective damages in tort.

The common law naming system was a liability regime. Anyone could use any name provided that they did not use it fraudulently. A person was free to call herself whatever she wanted, just as she was free to play a copyrighted song or drive on the street, provided she paid for any damages she caused.

In contrast, the current system seems more like a property regime, with the state owning all names. Individuals receive a "license" to use officially recognized names, i.e., the one on their REAL ID. In most important aspects of life, individuals cannot use any other name because, in effect, the government owns them. Individuals can petition to receive a new name via the formal name changing process, but no one may obtain a name outside of this process—or possess two names. Without indulging in paranoia, the current naming regime numbers individuals for the convenience of the state. They become objects of data, who are not permitted to change, to use a computer term, the "string" that identifies them.

Professors Calabresi and Melamed famously argued that transaction costs should determine whether to use a property or liability regime.[305] "The conventional approach that emerged from Calabresi and Melamed's classic article is that courts should rely on liability rules when transaction costs are sufficiently high that the relevant parties will not be able to reach a consensual arrangement for access to the resource in question."[306]

---

300. Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783, 786 (2007).

301. Calabresi & Melamed, *supra* note 31, at 1105.

302. *Id.*

303. *See id.* at 1107.

304. *See id.* at 1105–06.

305. *Id.*

306. Lemley & Weiser, *supra* note 300, at 786. This conclusion is often highly debated. *See, e.g.*, Ian Ayres & Paul M. Goldbart, *Correlated Values in the Theory of Property and Liability Rules*, 32 J. LEGAL STUD. 121, 135–36 (2003) (showing that liability rules, if based on average expected harm, conditional on the actual value of harm, can be more efficient than property rules);

Trademark law and common law naming systems offer a nice illustration of the choice between property and liability rules. Under trademark, a company "owns" its name. It can enjoin others who use it, and no one can use it without the company's permission.[307] Presumably, legislators and courts believed that the transaction costs of a business assuring that no one else use its name were sufficiently low, so the trademark property rules emerged.

In contrast, anyone can use a common law name provided she pays for any damages she causes via fraud. Presumably, in the early days of the common law, the transaction costs of giving property rights to names of millions of people were too great. Indeed, a property rule never seemed necessary because in most transactions, one did not need absolute assurance of identity. Rather, there is a sliding scale. Consumer transactions, medical treatment, bank accounts, secured interests, contracts, and loans all undoubtedly require a level of certainty of identity. The common law's liability regime allowed for enough certainty as needed without the great cost of a property regime.

Interestingly, due to computers and information technology, the cost of a naming system for all individuals is no longer so great, and the government has incurred the cost of building such a system. Personal names could be treated as trademarks. Individuals could own their name, and others cannot infringe upon it. Individuals could "buy" names from others or license others. The state would stay out. Of course, such a treatment would allow for pseudonymity.

But, even as technology has lowered transaction costs, making a property regime in names possible and even a market in names possible, government undermines such a market by in effect cornering it. The government has de facto ownership of all names and will not transfer them—unless one jumps through its hoops via a formal name change. A person can only have one name at a time. To use a name without the government's consent would be a crime as elaborated above.[308]

From a Calabresi–Melamed perspective, what is the advantage of this arrangement? Perhaps there is no advantage for individuals, and the federal government's gradual takeover of the identity field constitutes a governmental decision to end a "market" in names. As Judge Posner famously said, "When transaction costs are low, the market is, virtually

---

Abraham Bell & Gideon Parchomovsky, *Pliability Rules*, 101 MICH. L. REV. 1, 5–6 (2002) (arguing for a combination of property and liability); Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 HARV. L. REV. 713, 715 (1996) (presenting a model in which liability rules based on average expected harm are more efficient than property rules).

307. *See* 15 U.S.C. §§ 1114–16 (2012).

308. *See supra* Part II.

by definition, the most efficient method of allocating resources."[309] Criminal law constitutes an inherently "inefficient" "coercive transfer" that bypasses the market's voluntary exchange.[310] Criminal law exists to "discourag[e] market bypassing."[311]

Why would the government outlaw an efficient market in names when such a move would frustrate the often legitimate desires of individuals to have different names? The reason, in part, for ending the market in names proceeds from fear of terrorism, which as discussed above, prompted the passage of the REAL ID Act. And, to some degree, the end of the name market is a logical outgrowth of the welfare state, which for decades had been gradually accreting even more precise records of the citizenry. As this Article shows, the government finds it easier to distribute benefits and keep track of people if no market in names exists. Citizens are placed in easy-to-use filing cabinets—or computerized databases. But there is a cost. Many people *want* privacy for legitimate reasons. Further, *Patterson* illustrates that the government is not always above using identification to persecute political and religious dissenters.[312] The purpose of this Article is not to come down one way or the other on this basic political trade-off. Rather, it attempts to uncover the largely ignored legal mechanisms that have affected this trade-off and how these legal mechanisms can frustrate or further privacy.

## CONCLUSION

This Article demonstrates how a quietly growing body of law and regulation, which requires government-recorded name identification in virtually every aspect of life, constitutes a major privacy threat. This web of law and regulation threatens to render the Constitution's anonymity protection against compelled identity disclosure a de facto nullity.

This Article proposes that pseudonymity, as guaranteed by common law and the First Amendment, could offer privacy against this identification regime. This Article analyzes the yet nascent case law involving individuals' rights to demand government-issued identification under a pseudonymous common law name. Building on the principles of the common law name and the First Amendment, this Article concludes that under certain circumstances, individuals have the right to a pseudonymous government-issued identification. Beyond the practical implication of this insight, this Article engages in a theoretical analysis

309. Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM. L. REV. 1193, 1195 (1985).

310. *Id.* at 1195–96; *see also* Claire Finkelstein, *The Inefficiency of Mens Rea*, 88 CAL. L. REV. 895, 900 (2000) ("Posner argues that crimes are acts that are necessarily inefficient because they involve bypassing a voluntary market.").

311. Posner, *supra* note 309, at 1196.

312. 357 U.S. 449, 451, 466 (1958).

of personal names. It describes the silent shift from the common law liability regime to the current government-owned property regime and shows how this shift reflects major change in the relationship between the state and citizen.